Scaling Trust and Reputation Management in Cloud Services

Isaac Nyabisa Oteyo
School of Computing and Informatics Technology
Makerere University
Kampala, Uganda

Drake Patrick Mirembe
Uganda Technology and Management University
Kampala, Uganda

Paul Nampala
Regional Universities
Forum for Capacity Building in Agriculture
Kampala, Uganda

Abstract

Trust and reputation (TR) are critical considerations in the adoption of cloud services. However, there are challenges in managing TR among cloud service providers that trickle down to the service requesters. The trends used currently for TR management are ad hoc and mostly driven by need and different approaches for representing TR management in cloud services have been proposed. A hybrid of the various methods and models yields a near optimal solution for TR management in cloud services. The hybrid can be constructed from the pool of TR management options for cloud services, the different technologies applied in cloud management, and the impact factors for the different categories of cloud services. These technologies and categories of cloud services are presented in this paper. With the increased use of cloud services, there is an urgent need for explicit institutional arrangements that will help in monitoring and regulation to secure TR in cloud computing platforms and environments.

Keywords: Cloud computing, Internet, platforms, service oriented architecure

1 Introduction

Cloud computing, a service oriented architecture based on mobility and cloud technologies, has experienced spectacular increase in the amount of applications, services, platforms, data and the number of consumers seeking for cloud services (Mohammad & Mcheick, 2011; Kourtesis, Alvarez-rodríguez, & Paraskakis, 2014; Yanes, 2010). Since the inception and evolution (Dykstra & Sherman, 2012) of cloud services, trust and reputation have prevented firms from fully accepting cloud service platforms (Hwang & Li, 2010). This has been attributed to the fact that provisioning of cloud services is different from the traditional methods of information technology (IT) services (Prasad, Green, & Heales, 2014), and customers are stack to the idea of physically seeing their data storage locations. This implies that for the cloud systems to be fully accepted, service providers have to ensure security for the virtualized data centres, guarantee user privacy, and maintain data integrity.

To the ordinary consumer, the cloud platforms come disguised as the Internet with capabilities of providing a wide range of services. The emergence of cloud computing has created potential for a global inter-connected computing environment. The interconnected environment results from the convergence of service orientation, virtualization, and standardization of computing through the Internet. The services provided are not limited to time and space since they can be accessed over the network. Cloud computing offers increased computational capabilities that enable seamless and transparent use of resources residing in the cloud. The extension of cloud services to the mobile environment has yielded mobile clouds with the potential for enabling mobile terminals have access to powerful and reliable computing resources ubiquitously. However, security, privacy, and reliability remain challenges that have to be addressed.

These are challenges for the sole reason of how TR is represented in the cloud. For example, typical collusion can occur among service providers to influence a higher rating on the quality of services, security, and privacy of the cloud services. A user seeking for these services may end up opting for what might not be necessarily on offer.

The distributed and non-transparent nature of cloud computing makes its acceptance and success an obstacle (Habib, Hauke, Ries, & Mühlhäuser, 2012). Potential customers and users often have a feeling of having no control over their data and are not sure whether cloud service providers can be trusted; the reputation of service providers, data protection and privacy are issues of concern to them (Yigit, Gungor, & Baktir, 2014). For example, instances have occurred where credit card numbers for clients have been exposed when in actual sense they should be kept confidential. Establishment of trust and reputation in the cloud computing environment is a major issue in the success of cloud services. Cloud technologies evolve over time making computing highly dynamic. Thus, TR for a given service provider keeps on changing against the continuum of time. This paper therefore, focuses on scaling and ways of representing TR management in cloud services appropriately. The paper is best on results from a study premised on two questions, (a) How is TR represented in cloud services? and, (b) How is scaling perceived as a dimension in cloud services?

2 Methodology

A systematic review of available literature on TR management from leading digital libraries (Pranata, Skinner, & Athauda, 2012) was conducted. Some of the libraries and repositories that were used as sources for the scientific publications include Science Direct, Google Scholar, IEEE Explore, Citeseer X, and ACM digital library. Also, the review process extended to other electronic environments including among others Peer-to-Peer (P2P), e-commerce, distributed systems and grid computing. Deductive reasoning was used to draw conclusions based from the synthesized existing knowledge. The databases and repositories (Table 1) were identified based on the knowledge that they are known to contain published work on TR management and cloud services. Articles were downloaded from each database based on their relevance to the search terms. The search terms that were used included trust, reputation, trust and reputation management, cloud services, and scaling cloud services.

Table 1: Online sources searched for relevant materials

Database	Url
Science Direct	http://www.sciencedirect.com
Google Scholar	http://scholar.google.com
IEEE Explore	http://ieeexplore.ieee.org/Xplore/home.jsp
Citeseer X	http://citeseerx.ist.psu.edu/index
ACM Digital Library	http://dl.acm.org/

Publications were selected on the following criteria;

1. Peer-reviewed articles focusing on trust and reputation management for cloud services.
2. Articles that address representation of TR in cloud services.
3. Articles describing approaches to scaling TR management in cloud services.

3 Cloud Service Resources

Resources for cloud services may sit on a cluster of servers at different locations (data centres) and can even span across continents. Access to the resources by firms and individuals is on a rental basis; customers pay for services to the providers just like any other utility (Prasad et al., 2014). The utility way makes it affordable for firms and individuals to have access to the services (Jula, Sundararajan, & Othman, 2014). Some firms have built business empires around provision of cloud services e.g., Google, Amazon, Yahoo and Microsoft offer cloud services for different products. For example, Google and Microsoft have taken the cloud services further by providing a suite of free word processing and spreadsheet software applications over the browser. Also majority of email services are now based on the cloud. However, users of cloud services have no control over the technology and infrastructure that supports them. This is one of the underlying principles in the provision of cloud services and the onus is on the service provider to maintain trust and reputation.

4 Cloud Services

Current cloud services can be categorized into Database-as-a-Service (DaaS), Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS) (Abbadi & Martin, 2011).

The SaaS works as a model software deployment and delivers a single application hosted as a service, through the browser to many customers using a multi-tenant architecture. The investment, maintenance, and support cost for the customer on this service are almost negligible. Thus, SaaS has become so common for different applications and even found its application among enterprise resource planners (ERPs). The DaaS allows users to rent storage space for a period of time (Alhamad, Dillon, & Chang, 2011). Integration, privacy, and data security for these services solely lies on the service provider. The IaaS provides a more flexible model for service requesters preferring to have more control over their resources; SaaS provides tightly-focused services (Abbadi & Martin, 2011). Some firms have already built business models for exploiting PaaS and IaaS; the platforms and infrastructure are accessed on hire by requesters of cloud platforms and infrastructure. For instance, cloud storage permits users to have access to storage space hosted on the cloud via the Internet.

5 Deployment of Cloud Services

Deployment and placement of cloud services follow different models; private cloud, hosted private cloud, and public cloud or community cloud model (Abbadi & Martin, 2011). The model describes where the service runs. Private clouds are dedicated to firms, and are domiciled within the data centres of such organizations, whereas the hosted private clouds have dedicated services hosted by a third party, and are inaccessible to other organizations. Public clouds are hosted externally, and the services are shared among different organizations. Cloud services are provisioned on the basis of trust. However, the highly distributed and non-transparent nature of cloud computing presents a considerable obstacle to the acceptance of cloud services by consumers (Habib et al., 2012). Potential users often feel that they lose control over their data and are uncertain on whether cloud service providers can be trusted. Of utmost concern is the capability of cloud service providers. For example, many consumers are concerned about the storage locations for their data and who has access to that data (Habib et al., 2012). There is need for service providers to be dependable in establishing confidence in the consumers adopting cloud services. This in essence necessitates a clear understanding of the taxonomy of cloud services.

6 Taxonomy of Cloud Services

Figure 1 illustrates the taxonomy of cloud services. The classification is based on the roles each entity plays and the type of services offered to consumers. Top on the hierarchy are cloud providers (CPs); they offer services on the cloud e.g., DaaS, SaaS, IaaS and PaaS to consumers (Habib et al., 2010, 2012); in addition, they provide hosting of cloud computing infrastructure together with its management. Contextually, cloud resellers (CRs), cloud consumers (CCs), and cloud brokers (CBs) may perform the role of CPs.

The CCs fall in two broad categories; end consumers and cloud-based service providers. End consumers include business firms, governmental agencies, research, and educational institutions. They utilize cloud services without extending new services to others (Habib et al., 2010, 2012). Cloud-based service providers, develop business models around the service they offer and extend new services to the consumers hosted in the cloud. Cloud auditors (CAs) conduct independent evaluations of other cloud entities in regard to services, operations of information systems, performance and security of cloud implementations (Habib et al., 2010, 2012). Based on their recommendation, that borders reputation, consumers can establish a certain level of trustworthiness and dependability on cloud service providers. Cloud carriers (CCas) permit provisioning of services seamlessly through connecting different cloud entities (Habib et al., 2010, 2012). The CCas may provide telecommunication networks and resources for accessing cloud services. Network operators and Telcos form part of this category.

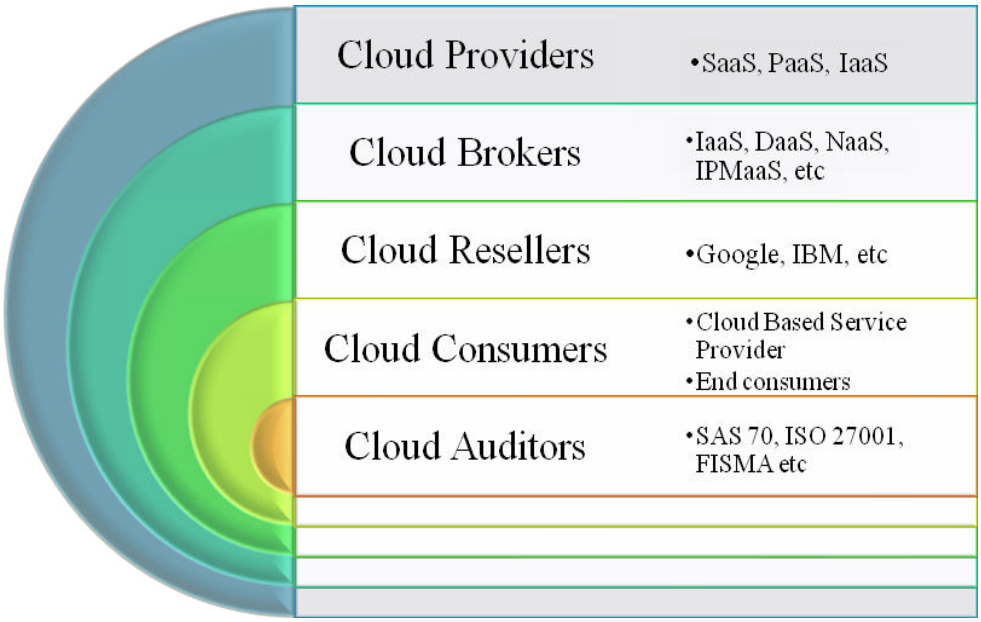

Figure 1: Taxonomy of cloud services (*Source* (Habib et al., 2012))

Cloud brokers (CBs) fall in two types; those that concentrate on building consumer relationships and service providers; they do not own or manage the cloud infrastructure. They provide services to potential CCs (Habib et al., 2010). Secondly, those brokers who extend additional services on top of the CPs' infrastructure. Thus, the CPs offering additional services like DaaS, IPMaaS, and NaaS, perform the role of brokers. Cloud resellers (CRs) offer services on behalf of cloud providers.

7 Applied Technologies in Cloud Management

Service level agreements (SLAs): These are agreements at the service level and are useful in quantifying what the cloud service provider is offering (Habib et al., 2012). The responsibility of monitoring SLA violations solely relies on the service requester. Unfortunately, most cloud service providers make SLAs as a defensive shield in case a customer takes any legal action on violation (Habib et al., 2010).

Auditing: Different audit standards, like ISO 27001, FISMA, and SAS 70 II are used to assure customers on the services and platforms on offer (Habib et al., 2012). However, standards on their own are not sufficient in alleviating cloud service security concerns.

Ratings and measurements: The ratings are done by current consumers of cloud services (Habib et al., 2012). Based on the customer feedback and technical measurements, the level of TR can be established to inform any prospective potential service requester (Deng, Huang, & Xu, 2014). Almost all cloud service providers give room for customer ratings and review, and use the feedback information collected to target prospective and potential clients. For social clouds, the rating can be based for example on the number of re-tweets (Weitzel, De Oliveira, & Quaresma, 2014).

Self-assessment questionnaires: These questionnaires provide a means for evaluating the core capabilities and competencies of cloud service providers (Habib et al., 2010, 2012). Issues of concern are very diverse among different cloud services consumers. Nonetheless, this self-assessments provide opportunity for feedback which has not been adequately utilized. This aspect constitutes areas for further research.

8 Related Work

Trust and reputation management has drawn attention among researchers. Problems associated with TR management such as aggregation algorithms and trust-based recommender systems have been studied in different contexts (Liu & Shi, 2010). Projects have been initiated to address transparency and trust establishment in cloud services e.g., Trustworthy clouds (TCloud) (Abbadi & Martin, 2011). This has allowed for proposed approaches for TR management. Some studies have shown that trust is a factor that mitigates risk in cloud services (Burda & Teuteberg, 2014).

Reputation-based trust management scheme is one such approach that is augmented by data and software watermarking techniques. The watermarking techniques protect shared data and distributed software modules (Hwang & Li, 2010). The aim for such approaches is to address dependability issues in the environment for cloud computing. Another approach suggests the use of trust-overlay networks over multiple data centres to implement a reputation system for establishing trust between cloud service providers and customers (Hwang & Li, 2010). Such techniques are proposed with the goal of securing multi-way authentications, enabling single sign-on, and enhancing access control to sensitive resources hosted in the cloud. Other studies have focused on different facets of TR management.

For instance, studies have been done on evaluation of cloud services that forms the basis for recommender systems in cloud services (Habib et al., 2012). However, these systems rely on assurance of trust between service requesters and cloud service providers. Trust, if well-established can help in overcoming some of the limitations associated with adopting cloud computing. Privacy and security challenges pose a unique set of issues that need to be addressed before adopting cloud services (Takabi, Zargar, & Joshi, 2013). It is important to provide secure and privacy aware communication processes within the cloud environment (Lin, Xu, Mu, & Wu, 2014). Customer evaluation of service providers is largely based on reputation and reliability which are derived from privacy and security. With recent developments in technology, provisioning of cloud services is now dynamic and flexible, but still faces fundamental challenges (Juan et al., 2012). In their study, they address the whole service life cycle and take a holistic approach to sustainable cloud service provisioning with the aims of reliable, sustainable and trustful cloud computing. Governance has a big stake in cloud services (Brandis, Dzombeta, & Haufe, 2014) especially in regard to its semantic aspects. The cloud is characterized by a high degree of information asymmetries between consumers and service providers. Quality of Service (QoS) and its management in cloud services has also provoked some interest for research (Kourtesis et al., 2014). This provokes concerns of re-defining the QoS in line with cloud services and designing scalable infrastructure for cloud services. Vast amount of resources are finding their way into the cloud environment; such resources need integration and proper management to yield the intended services to the customer. Also, securing cloud services and related potential problems has been explored (Nasir, Kiah, Khan, & Madani, 2013). This has been extended to measurement of trustworthiness for cloud service providers based on influence factors for quality of experience (QoE) (Ma, Hu, Yang, & Song, 2014) which require different ways for representing TR management.

9 Ways of Representing TR Management

The TR mechanisms have been applied in different fields including e-commerce, e-health systems, computer networks and social networks, which greatly rely on cloud computing services (Adewoyin & Vassileva, 2012). Some of the different ways as highlighted below have been researched and proposed for representing TR management in cloud services.

Formal Trust Model: This model was proposed by Prajapati, Changder, and Sarkar (2013). The model is based on SaaS and advocates for verification of the trust of service providers before consumers can access their services from the cloud. The model ensures trustworthiness of the service provider before accessing the service itself. It takes the proposition of modeling the trust management system based on space variant evaluation (Prajapati et al., 2013).

Multi-faceted TR Management Model: The model proposed by Habib *et al.* (2010), provides a means of identifying trustworthy cloud service providers based on compliance, data governance, and information security. With the model, TR is computed as a factor of competencies, capabilities, security measures, compliance with audit standards and customer support facilities of the service provider.

Service-oriented architecture (SOA)-TR Management Framework: This is based on the service oriented architecture (SOA) and uses web services to span several distributed trust management service nodes (Noor & Sheng, 2011). With the framework, cloud service consumers can give their trust feedback or inquire about certain cloud service's trust results using simple object access protocol (SOAP) messages. The framework is adaptive and highly scalable for constant collection of trust feedbacks and updating the trust results. The framework comprises of the service and service requester layers. The service layer is composed of IaaS, PaaS, SaaS, e-services, and the trust management service. Service requester layer consists of service consumers in the service layer.

Credibility model: This model proposed by Noor and Sheng (2011) takes into consideration the majority consensus and the feedback density.

For majority consensus, the expert judgement on the TR of a cloud service provider is considered. For feedback density, two issues arise; the total number of consumers giving trust feedback referred to as the feedback mass and the total number of feedbacks given for a cloud referred to as the feedback volume. Thus, the feedback density is expressed as a function of the feedback mass and the feedback volume.

Peer-to-peer reputation (P2Prep) protocol: This is a reputation-based protocol proposed by Aringhieri *et al.* (2006). The protocol focuses on peers keeping track and sharing reputations of their peers with others. This protocol works based on P2P cloud services. The network is polled for any available reputation information on selected cloud service providers.

10 Scaling TR Management

Scalability as a dimension for cloud computing can be increased by formulating secure cloud computations based on consistency-checking and TR (Khan & Hamlen, 2012). The aim is to leverage the distributed computing power of the cloud and strengthen its security.

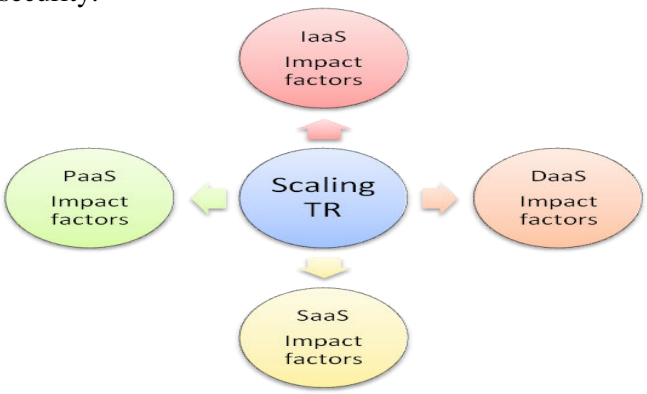

Figure 2: Scaling trust and reputation management

Figure 2 presents an illustration on TR scaling in relation to sources of impact factors that are dependent on the kind of service on offer. Each of the services provided by cloud computing has impact factors that determine its trust and reputation. Cloud technologies evolve with time, and as such have made cloud computing highly dynamic. This implies that, the TR for a given service provider keeps on changing against the continuum of time and calls for distributed computation of scalability. As new services are introduced in the cloud with time, the impact factors for scaling TR also increase. From the technology standpoint, the cloud infrastructure should be able to evolve with the new services introduced.

11 Conclusion

Different ways have been proposed for representing TR management in the cloud. Each of the approaches takes different elements to represent TR management. Thus, a hybrid of different ways would yield a more conclusive way of representing TR management. Given significant migration of computing services to the cloud and gradual increase in complexity of those services, there are challenges in managing TR among cloud service providers and service requesters. Incorporating a multi-disciplinary approach, TR management can benefit from careful integration and exploitation of advances in artificial intelligence, distributed computing, game theory and engineering; harnessing such advances can help create more reliable TR management systems. While scaling can be increased by formulating secure cloud computations, its aim is to leverage the underlying distributed computing power of the cloud as it strengthens security of cloud services.

This is coupled with the fact that scaling permits a service provider to widen the scope of services offered by the underlying computational capability. With the rapid spread of Web 2.0 applications, TR management approaches and systems play an important role in effecting cooperation among the distributed applications more so to the participants. To ensure total representation of TR management in cloud services, there is need for regulation, monitoring, and trust establishment in the cloud computing environments; more so, there is need for a third party assurance body to credit cloud service providers based on different parameters (e.g., response time, availability, and elasticity) that will ensure delivery of QoS to consumers. Besides scaling, TR takes different dimensions that include security, usability, and availability, that touch more on the service provider. This paper focused on ways of representing TR management and how scaling is perceived in cloud services.

Open issues have been cited and still remain of interest for future research. Some of the open issues include; establishing attack-resilient trust among nodes with no prior knowledge about each other, utilizing historical data in TR management and malicious manipulation of reputation-based trust, and exploiting reputation-based trust inference for building more reliable and large-scale Internet applications.

Acknowledgement

This publication has been produced with the assistance of the European Union. It is part of components of the senior author's engagements as a graduate student at Makerere University under the Intra-ACP Mobility program. The contents of this publication are the sole responsibility of the authors and can in no way be taken to reflect the views of the ACP Group of States or the European Union.

References

Abbadi, I. M., & Martin, A. (2011). Trust in the Cloud. *Information Security Technical Report*, *16*(3–4), 108–114.

Adewoyin, O., & Vassileva, J. (2012). Recommendation, trust and reputation management in a group online mentorship system. *CEUR Workshop Proceedings*, *872*, 53–58.

Alhamad, M., Dillon, T., & Chang, E. (2011). A Trust-Evaluation Metric for Cloud applications. *International Journal of Machine Learning and Computing*, *1*(4), 416–421.

Aringhieri, R., Damiani, E., De Capitani Di Vimercati, S., Paraboschi, S., & Samarati, P. (2006). Fuzzy techniques for trust and reputation management in anonymous peer-to-peer systems. *Journal of the American Society for Information Science and Technology*, *57*(1), 528–537.

Brandis, K., Dzombeta, S., & Haufe, K. (2014). Towards a framework for governance architecture management in cloud environments: A semantic perspective. *Future Generation Computer Systems*, *32*, 274–281.

Burda, D., & Teuteberg, F. (2014). The role of trust and risk perceptions in cloud archiving - Results from an empirical study. *Journal of High Technology Management Research*, *25*(2), 172–187.

Deng, S., Huang, L., & Xu, G. (2014). Social network-based service recommendation with trust enhancement. *Experts Systems with Applications*, *41*(18), 8075–8084.

Dykstra, J., & Sherman, A. T. (2012). Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques. *Digital Investigation*, *9*, S90–S98.

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*(19), 1–18.

Habib, S. M., Ries, S., & Mühlhäuser, M. (2010). Cloud computing landscape and research challenges regarding trust and reputation. In *Proceedings - Symposia and Workshops on Ubiquitous, Autonomic and Trusted Computing* (pp. 410–415).

Habib, S. M., Ries, S., Muhlhauser, M., & Varkkattu, P. (2010). Towards a Trust Management System for Cloud Computing Marketplaces: using CAIQ as a trust information source. *Security and Communication Networks*, *2*, 71–81.

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

Juan, A., Hernández, F., Tordsson, J., Elmroth, E., Ali-eldin, A., Zsigri, C., … Sheridan, C. (2012). OPTIMIS : A holistic approach to cloud service provisioning. *Future Generation Computer Systems*, *28*(1), 66–77.

Jula, A., Sundararajan, E., & Othman, Z. (2014). Cloud computing service composition : A systematic literature review. *Expert Systems with Applications*, *41*(8), 3809–3824.

Khan, S. M., & Hamlen, K. W. (2012). Hatman: Intra-cloud trust management for Hadoop. In *Proceedings of the International Conference on Cloud Computing* (pp. 494–501).

Kourtesis, D., Alvarez-rodríguez, J. M., & Paraskakis, I. (2014). Semantic-based QoS management in cloud systems : Current status and future challenges. *Future Generation Computer Systems*, *32*, 307–323.

Lin, H., Xu, L., Mu, Y., & Wu, W. (2014). A reliable recommendation and privacy-preserving based cross-layer reputation mechanism for mobile cloud computing. *Future Generation Computer Systems*, 6–10.

Liu, L., & Shi, W. (2010). Trust and Reputation Management. *Internet Computing*, *14*, 30–33. http://doi.org/10.1109/MIC.2010.124

Ma, H., Hu, Z., Yang, L., & Song, T. (2014). User feature-aware trustworthiness measurement of cloud services via evidence synthesis for potential users. *Journal of Visual Language and Computing*, *25*(6), 791–799.

Mohammad, A. F., & Mcheick, H. (2011). Cloud services testing: An understanding. In *Internation Conference*

on Ambient Systems, Networks and Technologies (Vol. 5, pp. 513–520).

Nasir, A., Kiah, M. L. M., Khan, S. U., & Madani, S. A. (2013). Towards secure mobile cloud computing : A survey. *Future Generation Computer Systems*, *29*(5), 1278–1299.

Noor, T. H., & Sheng, Q. Z. (2011). Credibility-Based Trust Management for Services in Cloud Environments. In *International Conference on Service-Oriented Computing* (pp. 328–343).

Prajapati, S. K., Changder, S., & Sarkar, A. (2013). Trust Management Model For Cloud Computing Environment. In *Proceedings of the International Conference on Computing, Communication and Network* (pp. 1–5).

Pranata, I., Skinner, G., & Athauda, R. (2012). A holistic review on trust and reputation management systems for digital environments. *International Journal of Computer and Information Technology*, *1*(1), 44–53.

Prasad, A., Green, P., & Heales, J. (2014). On governance structures for the cloud computing services and assessing their effectiveness. *International Journal of Accounting Information Systems*, *15*(4), 335–356.

Takabi, H., Zargar, S. T., & Joshi, J. B. D. (2013). Security, Privacy and Trust Management Mobile Cloud Computing and Its Challenges. In D. B. Rawat, B. B. Bista, & G. Yan (Eds.), *Security, Privacy, Trust, and Resource Management in Mobile and Wireless Communications* (pp. 384–407). IGI Global.

Weitzel, L., De Oliveira, J. P. M., & Quaresma, P. (2014). Measuring the reputation in User-Generated-Content systems based on health information. In *International Conference on Computational Science* (Vol. 29, pp. 364–378). Elsevier Masson SAS.

Yanes, A. (2010). Reputation in Cloud Computing. In *Network Security*. Retrieved from http://www.cse.hut.fi/en/publications/B/11/papers/yanes.pdf

Yigit, M., Gungor, V. C., & Baktir, S. (2014). Cloud Computing for Smart Grid applications. *Computer Networks*, *70*, 312–329.