CURRENT RESEARCH IN
COMPUTER SCIENCE
ISSN 2788-7707
MAY. 2021 VOL. 1, NO. 1

Research Quantitative Trust Models Using Cloud Security as a Quantitative Framework for Trust Metrics

Muchahari McKnight, Sanchez-Rola
School of Computing and Informatics, University of Nairobi, Nairobi, Kenya

ABSTRACT

The uptake of cloud services is pegged mainly on the level of trust cloud users have in the cloud computing solutions offered. Whereas trust is subjective, it can be modeled quantitatively thereby introducing objectivity, through a scientific method, in the process of determining the presence or absence of trust. The proposed quantitative model, introduced a new metric for measuring trust, confidence interval, which is derived from a comparison of results from service provider integrated QoS measuring tools, and a vendor neutral QoS monitoring tool, which run simultaneously in the background while the user is utilizing the cloud provider's services. The fact that the model relies on results from a vendor neutral tool, which are compared with the cloud provider's integrated tool, makes the tool more reliable and effective than those based on one set of results. This paper was however limited by the fact that only one metric, service availability, was used in comparison due to limitation on the number of metrics monitored by the cloud provider's tools. To enhance the trust comparison capabilities, Cloud providers could incorporate other quantitative metrics like service response time and service stability into their integrated QoS monitoring tools. Modeling of quantitative trust continues to be a live field of study, this paper therefore enhances the ongoing research.

KEYWORDS

Trust; Trust value; Modeling; Cloud computing; Confidence interval; Vendor neutral; QoS.

1. Introduction

The uptake of any technological innovation depends on whether the end users of the technology have trust in the solutions fronted by that technology. This consequently means end user trust in systems is a vital determinant of the success of that system. This calls for a clear definition of trust in the context of Information Systems and scientific means to enable measuring the trust level of users in particular systems.
Various definitions of trust have been presented, namely, accepted dependence on a system occasioned by the ability of the system to deliver services that are dependable [1]; willingness to depend on and be vulnerable

to an Information System in uncertain and risky environments [2]; the subjective probability by which an individual, A, expects that another individual, B, performs a given action on which its welfare depends (Reliability trust) [3]; the extent to which one party is willing to depend on something or somebody in a given situation with a feeling of relative security, even though negative consequences are possible (decision trust)[4]; and a state of expectations resulting from a mental reduction of the field of possible [5].

From the fronted definitions, certain terms are conspicuously present, namely, dependence, reliability and expectations. This paper therefore, putting into consideration the definitions and key terms appearing in other definitions defines trust as, the level of confidence a user has in an Information System. This level of confidence is very key in determining the uptake of the Information Systems and thus pivotal in their success or failure.

To be able to measure trust, measurable metrics have to be identified, and a measurement model has to be developed. For the measurements to be scientific, they must satisfy key characteristics of a scientific research method, namely, logical and repeatability [6], with no room for inherent subjectivity in the model. This paper presents work that addresses the problem of systemic subjectivity in the existing trust measurement models.

The field of trust metrics is a well studied field and has yielded several metrics that can be used in measuring trust. The metrics include: availability exhibited by readiness for correct service; reliability showed by continuity of correct service; safety confirmed by absence of catastrophic consequences on the user(s) and the environment; integrity depicted by absence of improper system alterations; and maintainability established by ability to undergo modifications and repairs [1].

Other metrics, classified as QoS metrics include Execution Time, which is the time taken by a service to execute and process its sequence of activities; Latency, defined as delay time between sending a request and receiving the response; Response Time, described as time required to process and complete a service request; Throughput, referred to as number of requests a service can process per unit of time; Availability, defined as probability that a service is up and accessible to use and Reliability, which is ability of a service to perform its function correctly with either 'no fail' or 'response failure to the user' [7].

Whereas the metrics are sufficient and well defined, as highlighted by Avizienis et al [1] and Zainab et al [7], the models on which the metrics can be used are lacking in objectivity that can lead to scientific trust values. An objective model is therefore required that can clinically compute trust values for information systems.

2. Related Work

Cloud computing has been known to tremendously reduce the investment as well as the operating costs of firms, both established and startups. Despite this knowledge, firms are reluctant to fully adopt cloud computing despite the beneficial impacts siting reasons such as security, privacy and trust [8]. This paper focuses on trust as an issue to be addressed to spur the uptake of cloud services.

Since trust can be used as a determinant metric in cloud provider selection, it has to be measurable for its admissibility in cloud provider selection contexts [9]. This underscores the need for scientific modeling of trust using the various trust metrics, for the trust values to be credible. The factors that form a basis for cloud trust establishment between the cloud providers and their clients include QoS, SLAs, publicly available reviews, audits based on established standards and Client support [9].

Various trust measuring in cloud computing have thus been modeled around QoS, SLAs, user reviews and Audits based on established standards. Due to the critical role trust plays in cloud provider service selection, it is equally important to have credible trust measuring models. The various existing models are therefore critically reviewed in this paper with a view of documenting identified shortcomings and possible solutions.

2.1 Qos Trust Model

A trust computation model that utilizes availability, reliability, turnaround efficiency, and data integrity as metrics was proposed by Manuel [10].
The availability of a given resource ( ) is computed as a ratio of the accepted jobs against the total number of jobs submitted per given time period.
total accepted jobs

Due to the fact that the model developed by Manuel [10] uses QoS parameters, it is known, as QoS trust Model. The main shortcoming of this model is the subjective manner of assigning weights used in computing the final trust value. The weights are assigned based on an individual's priority or preference, thus introducing subjectivity.

2.2 Cloud Security Dependency Model

A quantitative framework for accessing cloud security, using a dependency model that validates both the offered services and customer's requirements validated by checking service conflicts and different Service Level Obligation compatibility issues, is proposed by Taha [12].

The proposed dependency model is composed of five stages, namely, Security requirements definition, Requirements Quantification, Dependency management approach, Structuring security SLA services using Dependency Structure Matrix and Cloud Service Provider Evaluation.

The proposed framework and model suffers from the limitation of the fact that customers are only able to trust the result of the proposed assessment as long as the information taken as input is reliable [12].
This calls for the use of an independent auditor to perform a third-party attestation of the cloud provider's security SLA through a scheme such as the Cloud Security Alliance Open Certification Framework, as well as the fact that the model is limited to security aspects of the cloud services only.

2.3 Composite Trust Metric Model

A composite trust metric, consisting of impression and confidence was introduced by Yefeng et al [13]. The authors advance the fact that trust can be constructed by algorithms through observing past events, such as positive or negative evidence or feedback on social platforms.

The proposed framework [13] is based on measurement theory, Dempster –Shafer belief theory and error propagation theory. The framework has three phases, namely trust modeling, where trust related information is mapped on trust metrics. For example, reviews and proposition from users of epinions.com, likes and dislikes from users of Facebook.

The second phase is trust inference, which focuses on propagating and aggregating the obtained trust metrics over the whole network or over the part of interest, while decision making using the measured trust is the final phase.

The widely used metrics for representations of trust are binary metrics, scaled metrics, probability based metrics and similarity based metrics are used [13].

The proposed framework uses a model expressed as: T (m, c), where m measures how trustworthy the trustee is in the truster's point of view, while, confidence c measures how confident the truster is about the evaluation of impression/trustworthiness m.

The modeling for the trust values for the epinios.com platform is computed as: For a trust relation from user A to user Z, the impression m is the average of ratings that A rates Z's review articles. It is then converted into value in [0, 1] as:

$$m_{Z}^{A} = \frac{\sum_{i=1}^{i=N} \text{Rating}_i}{5*N}$$

For twitter, interactive tweets are used to build trust using sentiment analysis. Using sentistrength, an analysis is constructed for each tweet, which gives a discrete value from −4 to +4 for each tweet.

This is then converted into discreet values into the interval [0, 1], using the equation:

((Sentiment+4)/8).

Whereas this model develops measured values for trust, it is a highly subjective process. The reviews, likes, dislikes are all assigned by users based on their perceptions, moods, social cultural inclinations and subjective interpretations. These user perceptions are likely to change with time, or as new information emerges and are thus not objective hence not suitable for use in scientific modeling.

3. Methodology

The approach used in designing and experimenting with the proposed trust quantification model is premised on the fact that cloud computing solutions have embedded capabilities to monitor and measure QoS. The capability measures QoS as provisioned by the provider, the results are then available for users to query from the providers' systems. A comparison can thus be made with the results from the same cloud platforms obtained using a vendor neutral QoS monitoring model developed by Makokha et al [14], which measures QoS across all cloud providers. This comparison can then be modeled quantitatively.

The vendor neutral model was developed as a browser extension and installed on chrome, using chrome's extension loading module as depicted in figure 1.

The developed vendor neutral model is limited to Software as a Service (SaaS) cloud solutions and therefore this paper also limited its scope to SaaS solutions only.

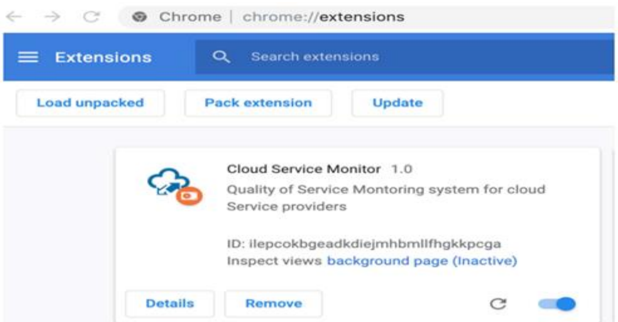

Figure 1. Integration of Vendor Neutral QoS Model into Chrome.

Chrome was chosen because it is the most widely used browser with the highest number of extensions developed for it [15]. After integration, the user continues to use chrome to execute the tasks identified for experimentation while the QoS model runs in the background.

Using the vendor neutral model, the experimentation process involved creating user accounts on the cloud provider's platform and using the platform in a way that an ordinary user would use the services. The platforms chosen were Google docs and Microsoft 365, the major cloud providers with similar products that can be easily compared [16].

The experimentation tasks involved opening, using, closing and re opening Word, Excel and Power Point applications from the two providers, which were opened on different tabs of the same browser. During experimentation, the vendor neutral tool was monitoring the QoS values, namely, service response time, service availability and stability, conversely, the cloud provider's tool was also monitoring the QoS values.

Using the results from the vendor neutral cloud QoS Monitoring solution, and applying the most widely used confidence interval of 95% [17], on the results from the vendor neutral tool, and comparing them with the results from Google and Microsoft QoS tools, a quantification trust model was built based on how close or far the results are from each other. The comparison is also enhanced by the user experience during usage of the services.

4. Trust Quantification in Cloud Computing

To address the challenges of the highlighted quantitative trust measurements in computing systems, this paper proposes a quantitative metric, confidence interval, for measuring trust in computing platforms, especially cloud computing environments.

The necessity for trust measurement in cloud solutions is premised on the fact that trust is considered a non functional property of a service that can be used in service selection, in cases where there are similar services on offer [7].

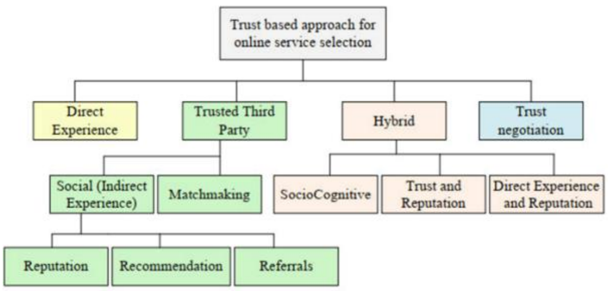

Figure 2. Trust approaches for online service selection.

The service selection approaches based on trust can be through direct experience, Third Party Trust, a Hybrid approach and Trust Negotiation [18]. These approaches are depicted in figure 2.

Noting that trust is a dynamic concept, it can be divided into three development phases: trust building, where trust is formed; stabilizing trust, where trust already exists; and dissolution, where trust ends [19].

The model proposed in this paper enhances the concept of direct experience trust [18] and trust building process [19].

4.1 Quantitative Trust Model for Cloud Computing Solutions

To address the highlighted shortcomings in existing trust models, our proposed model is pictorially represented in figure 3.

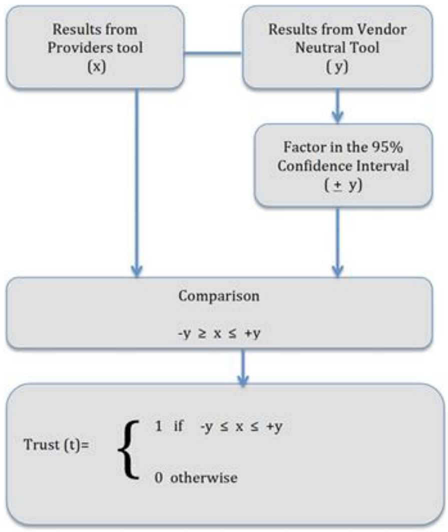

Figure 3. Proposed Trust Quantification Model.

4.2 Quantification of Trust in Major SaaS Cloud Providers

The metric used in comparison of the results was service availability because it is a common metric measured by both the vendor neutral model and the cloud providers' integrated QoS monitoring tools. The results from the experiment are as tabulated in table 1.

Table 1. QoS Results from Vendor Neutral Tool.

Platform Average

Platform	Average Response Time	Average Availability	Stability
Google	4.39	100%	Stable (1.986 sec)
Microsoft	5.99	100%	Stable (5.845 sec)

From the analysis in table 1, the average service response time, time required to process and complete a service request, for Google is 4.39 seconds while for Microsoft is 5.99 seconds. Both platforms had availability, probability that a service is up and accessible to use, of 100% since at no time during experimentation did any of the platform report a platform failure leading to outage of services.

Whereas the availability is 100%, the stability, fluctuations in the service response time, computed using standard deviation, are higher for Microsoft at 5.845 seconds than for Google at 1.986 seconds, meaning the Google platform was more stable than the Microsoft platform.

From the studies done by Makokha et al [14], a common metric between the vendor neutral cloud QoS monitoring model and the cloud provider integrated QoS monitoring tools is the service availability.

Similarly, Microsoft, through its QoS monitoring platform, https://admin.microsoft.com, showed the status of office suites to be healthy during the entire time, translating to 100% availability.

The QoS value screenshots from the vendor neutral model for Microsoft and Google platforms are as shown in figure 4 and 5 respectively.

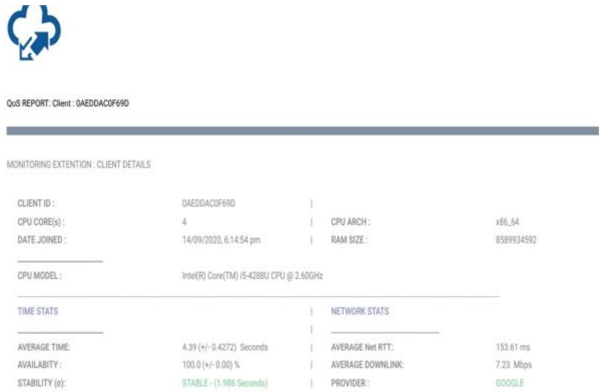

Figure 4. Microsoft Office QoS Results.

Figure 5. Google Docs QoS Results.

Using the proposed quantitative trust model, and service availability which is the common QoS Metric between the vendor neutral tool and cloud providers' integrated tools, trust can be computed as in table 2.

Table 2. Modeling Quantitative trust.

Platform	Vendor Neutral results	Cloud Provider Results	Trust Value
Google	100%(± 0)	100%	1
Microsoft	100%(± 0)	100%	1

From table 2, a cloud user can trust the results from the cloud providers due to the fact that they are within the confidence interval of the vendor neutral tool.

This is critical for the trust building phase as highlighted by Grabner-Kräuter et al [19], and also augments the direct experience concept advanced by Dragoni [18] since the user will have experienced the services from the providers during the experimentation phase.

5. Conclusions

The uptake of cloud services is pegged mainly on the level of trust cloud users have in the cloud computing solutions offered. Whereas trust is subjective, it can be modeled quantitatively thereby introducing objectivity, through a scientific method, in the process of determining the presence or absence of trust.

The proposed quantitative model, introduced a new metric for measuring trust, confidence interval, which is derived from a comparison of results from service provider integrated QoS measuring tools, and a vendor neutral QoS monitoring tool, which run simultaneously in the background while the user is utilizing the cloud provider's services.

The fact that the model relies on results from a vendor neutral tool, which are compared with the cloud provider's integrated tool, makes the tool more reliable and effective than those based on one set of results.

This paper was however limited by the fact that only one metric, service availability, was used in comparison due to limitation on the number of metrics monitored by the cloud provider's tools.

To enhance the trust comparison capabilities, Cloud providers could incorporate other quantitative metrics like service response time and service stability into their integrated QoS monitoring tools.

Modeling of quantitative trust continues to be a live field of study, this paper therefore enhances the ongoing research.

References

Avizienis, A., Laprie, J., Randell, B. and Landwehr, C. Basic Concepts and Taxonomy of Dependable and Secure Computing. IEEE Transactions on Dependable and Secure Computing, Vol. 1, No. 1, 2004.

Gefen D, Benbasat I, Pavlou P. A research agenda for trust in online environments. Journal of Management Information Systems 24 (4): 275-286, 2008.

Gambetta, D. Can We Trust Trust? In D. Gambetta, editor, Trust: Making and Breaking Cooperative Relations, pages 213-238. Basil Blackwell. Oxford, 1990.

McKnight, D. H. and Chervany N. L. The Meanings of Trust. Technical Report MISRC Working Paper Series 96-04, University of Minnesota, Management Information Systems Research Center, 1996.

Bako R. A view of trust and information system security under the perspective of critical infrastructure protection. Revue des Sciences et Technologies de l'Information - Série ISI: Ingénierie des Systèmes d'Information, Lavoisier, 2017, 22 (1), pp. 109.

Bhattacherjee, A. Social Science Research: Principles, Methods, and Practices (2012). Textbooks Collection. 3. http://scholarcommons.usf.edu/oa_textbooks/3.

Zainab, A., Perry, M. and Capretz, M. A (2011). Trust Metrics for Services and Service Providers in The Sixth International Conference on Internet and Web Applications and Services ICIW 2011 March 20-25, 2011 - St. Maarten, The Netherlands Antilles.

Habib, S., M., Ries, S. and Muhlhauser, M.(2010) Cloud computing landscape and research challenges regarding trust and reputation, in Proceedings of the 2010 Symposia and Workshops on Ubiquitous, Autonomic and Trusted Computing. IEEE Computer Society, 2010, pp. 410-415.

Manuel, P. A trust model of cloud computing based on Quality of Service. Annals of Operations Research, Volume 205, 2013.

Nagat, D., Jamal B. and Hongyang Q. Computationally Grounded Quantitative Trust with Time. Proc. of the 19th International Conference on Autonomous Agents and Multiagent Systems (AAMAS 2020), B. An, N. Yorke-Smith, A. El Fallah Seghrouchni, G. Sukthankar (eds.), May 9-13, 2020, Auckland, New Zealand. 2020.

Taha, A. (2018) Quantitative Trust Assessment in the Cloud. MSc, Technische Universit?t Darmstadt, Germany.

Yefeng R., Ping Z., Lina A. and Arjan D. Measurement Theory-Based Trust Management Framework for Online Social Communities. ACM Transactions on Internet Technology, Vol. 17, No. 2, Article 16, Publication date: March 2017.

Makokha, F., Opiyo, E. and Chepken, C. Browser Integrated Vendor Neutral Cloud QoS Monitoring System. International Journal of Computer and Information Technology, Vol 8, No 6 (2019).

Hazra, A. Using the Confidence Interval Confidently. Journal of Thoracic Disease, Volume 9 Issue 10, 2017.

Dragoni, N. Toward trustworthy web services - approaches, weaknesses and trust-by-contract framework. IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology, Volume 3, pp. 599-606, 2009.

Grabner-Kruter, S. and Kaluscha, A. E. (2008). Consumer trust in electronic commerce: Conceptualization and classification of trust building measures, in Teemu K. and Heikki K. (Eds.) Trust and New Technologies. Edward Elgar Publishing 2008, Cheltenham, United Kingdom.

Copyrights