Journal of Computers Vol. 29 No. 6, 2018, pp. 235-242
doi:10.3966/199115992018122906023

User-oriented Cloud SLA Assurance Framework

Le Sun[1*], Chen Wang[1], Jinyuan He[2], Hai Dong[3], Jiangang Ma[2], and Yanchun Zhang[2]

[1] School of Computer Software, Nanjing University of Information Science and Technology, Nanjing, China
sunle2009@gmail.com, wangchennuist@126.com

[2] Institute for Sustainable Industries and Livable Cities, Victoria University, VIC, Australia
jinyuan.he@live.vu.edu.au, {jiangang.ma, yanchun.zhang}@vu.edu.au

[3] School of Science, RMIT University, VIC, Australia
hai.dong@rmit.edu.au

Received 9 January 2018; Revised 17 January 2018; Accepted 22 January 2018

Abstract. Cloud computing technology presents new challenges in terms of service provisions and consumptions. One of the key issues in this area is to guarantee an agreed level of cloud services to service users. One way to cope with this challenge is to ensure the commitment of Service Level Agreements (SLAs) in which the level of services is formally defined. Although in the literature a number of studies have been carried out on SLA assurance, the majority of them aims to improve the ability of SLA adherence of service providers and focus on minimizing the losses of both parties in a service transaction. However, having such a service-provider-oriented SLA assurance framework is not effective to service users as it is focused mainly on ensuring the benefits of service providers. In this paper, a comprehensive framework will be developed from the service users viewpoint to analyse the ability of SLA commitments of both service providers and service users and ensure the profits of service users by two key steps: (1) design a methodology of transactional risk assessment to assist in selecting qualified services; and (2) devise a SLA monitoring mechanism to monitor SLA enforcement and predict possible SLA violations over the lifetime of a service instance. In particular, the proposed approach will take into account resource performance and network status in the SLA monitoring mechanism as they both have significant effects on successful delivery of services to service users.

Keywords: cloud service, performance monitoring, SLA assurance, user-oriented service selection

1 Introduction

Cloud computing with its features is an attractive option for both service providers and service users. From the perspective of service users alone, it eliminates the need to pre-plan and allows the infrastructural resources to be used as services from different vendors at their desired point in time on a demand and pay-as-you-go basis at much lower premiums. To ensure the delivered service meets the desired level of qualities, service level agreements (SLAs) [1] between the service users and service providers are established. SLAs are multi-faceted agreements that provide a clear understanding of the expected services thereby eliminating unrealistic expectations, plan for the optimal use of resources, and maximize the revenue to be generated. Non-adherence to SLAs is costly to the service users in many ways. For example, the non-achievement of the expectations at the required time which may be critical for their needs may produce undesirable consequences.

To avoid such undesired scenarios, a more proactive approach to SLA management is needed. In other words, an intelligent framework is needed, which in real time assists the service users at different stages of the SLAs, from their formulation to their commitment, to ensure their compliance and assurance. Although significant work has been done on SLA assurance in cloud computing, most of them focus on

* Corresponding Author

solutions of issues oriented by service providers, such as resource adaptation based on SLA monitoring information [2-3], SLA portfolio management [4], etc. Limited work has gone into SLA assurance from the perspective of service users. Thus, an intelligent framework for SLA assurance will be developed in the proposed work, titled as User-Oriented SLA Assurance (UOSA) framework, and is intended to guarantee SLA assurance for service users and consequently minimize the possibility of loss in a service transaction. It will assist the service users both in pre and post interaction-start time phases. The key issues that should be highlighted in these two stages are described as follows.

In the pre-interaction-start time phase, service users need to make an informed decision about the selection of services, in the belief that the service provider is capable of providing services to meet their requirements in terms of both quality and functions. An effective way is to identify the SLA-violation risk before entering into an interaction with a provider. In the literature, approaches have been proposed to achieve this by using techniques such as trust or reliability [5]. In the proposed approach, the notion of transactional risk will be investigated and used to assist service users in selecting qualified cloud services.

In the post-interaction-start time phase, it is hoped that during the process of service consumption, real-time monitoring of SLA enforcement status and detection of potential SLA violations should be made available to cloud service users in a seamless way. Thus, an SLA monitoring and violation prediction mechanism is devised in this framework, by which SLA is monitored from two aspects: resource performance and network status. The monitored data is collected and analysed regularly, based on which a sophisticated prediction algorithm is designed and used to predict possible SLA violations. Finally, the monitoring report and rational solutions for SLA violations are presented to service users.

The significances of this work are as: (1) Lacity et al. [6] pointed out that organizations are increasingly sourcing their business processes, which is even getting more significance in cloud computing industry. In such circumstances, the selection of cloud service providers with outsourced services presents increased challenges to the service users. This project will introduce techniques that can help service users to analyze the transactional risk and select capable cloud service providers. (2) The framework of SLA monitoring will provide exact and detailed information of SLA commitments by providers for service users to help them effectively control and maintain their applications on the cloud platform. (3) The techniques for system performance forecasting will enhance the accuracy of prediction of SLA violations in complex and dynamic systems. (4) This project will enable service users to detect and predict SLA violations proactively by proposing techniques that determine beforehand the chances and consequences of the occurrence of SLA violations, which will help them to develop decisive strategies to minimize losses.

The rest of this paper is structured as follows: Literature review is discussed in Section 2. Research methodologies and approaches are discussed in Section 3. Section 4 described how to evaluate the UOSA system. Section 5 concludes this paper.

2 State-of-The-Art of SLA Assurance

The work of transactional risk assessment in pre-interaction-start time Phase is discussed from two aspects: (1) SLA-based risk assessment from the perspective of service provider; (2) SLA-based risk assessment from service users' perspective.

SLA-based risk assessment from the perspective of service provider. Various approaches were proposed for service provisioning decisions of service providers when establishing SLAs [7-8]. Anya et al. [9] proposed an adaptive cloud service provisioning algorithm. They designed a predictive analytics engine for managing elasticities of cloud services by mining the history of SLA compliance and the knowledge of business transactions. Katsaros et al. [10] designed a service provisioning framework, namely SLA as a Service (SLAaaS), to detect SLA violations and enhance the robustness of cloud infrastructures for service providers. Ardagna et al. [11] presented an online resource management algorithm based on game theory. The proposed algorithm allocates IaaS resources to a number of SaaS providers, which achieves an optimal trade-off of revenues and penalties of resource allocation failures. Hussain et al. [12] proposed an approach to guarantee the expected QoS levels of cloud services by considering different kinds of quality factors in real time. In order to quantize the risk and thereby make the evaluation of the service delivery more precise, Michalk et al. [13] presented a novel approach that enables service providers to select a particular combination of SLAs which can minimize the risk of SLA violations. The proposed techniques for measuring risk are based on the decision theory. Utility theory

and the concept of risk aversion are employed to express a decision maker's preference.

SLA-based risk assessment from service users' perspective Existing research is dedicated to the uncertainty of consumer's belief in the ability of the provider to meet service expectations [14]. In particular, Wu et al. [15] introduced a customer driven cloud resource provisioning algorithm to balance resource cost and customer service levels based on SLA assurance. The proposed algorithm handles heterogeneous infrastructure level resource provisioning and users' requests of enterprise cloud systems. However, they did not demonstrate the influence of risk on the transaction decision process. The difference between and dependence on trust and risk were discussed in [16]. Abdullah et al. [17] also contributed to the achievement of consumers business expectations. They discussed the problem of uncertainty within service provisioning offer, and provided a measure of tolerance towards uncertainty by creating Bayesian Decision Models. In this way, capable service providers can be selected to guarantee SLA commitment during service provisioning. Although this work analysed transactional risk for consumers from the perspective of SLA violation, it did not create a complete transactional risk assessment system for qualitative and quantitative measurements of risks. Ren et al. [18] presented a data possession scheme that is mutually verifiable and provable. The proposed method builds the homomorphic authenticator by using the Diffie-Hellman shared key.

SLA monitoring strategies as well as detection and prediction of possible SLA violations were actively studied and developed in service-based environments.

SLA monitoring strategies in post-interaction-start time phase. Cloud BOSS [19] is introduced as a service-assurance-oriented platform to manage and guarantee the level of service quality in the cloud. Instead of measuring QoS (Quality of Service) to guarantee service delivery to users, the authors focused on the measurements of QoE (quality of experience) of service users by mapping KPIs (Key Performance Indicators) to KQIs (Key Quality Indicators) to meet requirements in SLAs. The proactive monitor in this framework is intended to predict SLA violation by setting a warning threshold. It is worth mentioning that the authors took customer experience into consideration to implement end-to-end SLA assurance and were planning to investigate techniques to perform quality tests from the customer's perspective. Romano et al. [20] presented a dependable QoS monitoring facility named Quality of Service MONitoring as a Service (QoS-MONaaS). Rather than gathering monitoring data at intervals of minutes, QoS-MONaaS uses a stream processing computing technology, which makes continuous monitoring - and ultimately timely response -possible. QoSMONaaS focuses on the performance delivered at the business process level to reflect the real interests of service users. Ciciani et al. [21] described the key design choices underlying the development of Workload Analyser (WA), a crucial component of the Cloud-TM platform which is a self-optimizing transactional data platform for the cloud. WA is capable of monitoring and categorizing resource consumption data. Based on these data, time-series-based analysis to forecast future trends of the workload fluctuations is implemented relying on R free software project [22]. WA allows the prediction of SLA violation and enables service users to have full control over what they want to be notified about. Oliveira et al. [23] designed an architecture for monitoring and accounting SLA deviations of networks. The proposed architecture is deployed in the form of an open source engine. Garg et al. [24] proposed a mechanism for admission scheduling and control by maximizing the profits and performance of resource allocation, and guaranteeing the SLAs. Serrano et al. [25] proposed a cloud model: SLAaaS that ensures the meeting of SLA requirements of cloud services, and can be applied to any type of cloud models. Ibrahim et al. [26] present an SLA assurance framework to guarantee SLAs for both cloud service providers and service users. In addition, Liu et al. [27] introduced a Parallel Deadline Guaranteed (PDG) scheme to optimize data allocation based on a bottom-up mechenism.

3 User-Oriented Service Level Agreement Assurance Framework

We develop a service-user-oriented SLA assurance framework, named UOSA framework, which is able to assist service users in ensuring SLA commitments by service providers. UOSA consists of two main stages, the service selection stage and the SLA monitoring stage. In the service selection stage, suggestions on the choices of suitable cloud services will be provided by assessing transactional risk based on the analysis of tailor-made SLAs. In SLA monitoring stage, the tailormade SLA will be monitored and rational suggestions will be given when an SLA violation is detected or predicted. Fig. 1

shows the diagram of the UOSA framework, in which sub-steps are labelled indicating the information flow. Three phrases are designed to implement this framework.

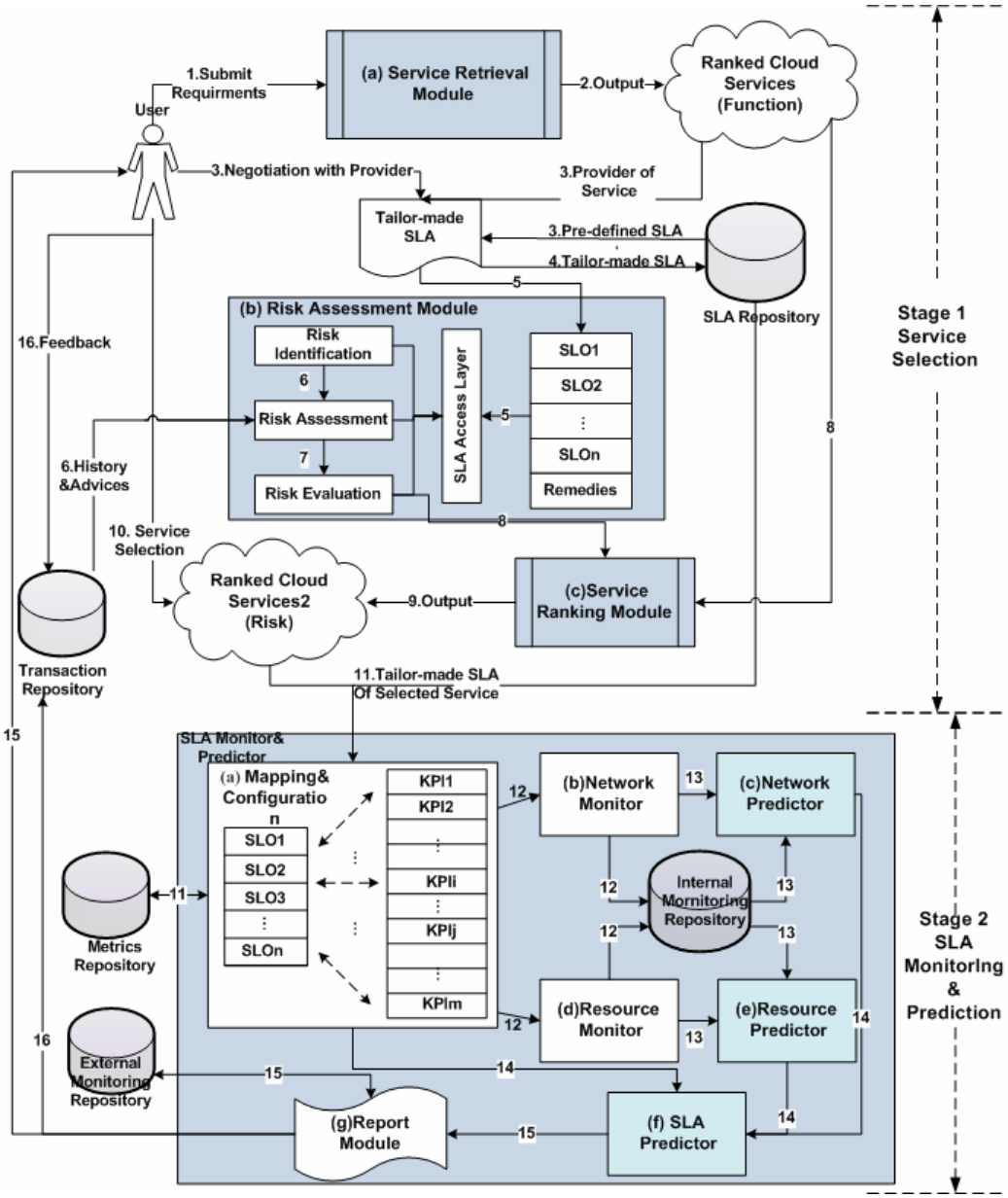

Fig. 1. User-Oriented SLA Assurance (UOSA) framework

Stage 1. Knowledgebase (KB) design. KB is an information repository in which valuable information for the service selection and SLA monitoring is stored and will be updated dynamically. Specifically, five kinds of information repositories are included in KB:

- Service repository. Service information published by service providers will be retrieved and will serve for the service retrieval module, based on which service users can query expected cloud services. This repository is included in the service retrieval module and is not displayed in Fig. 1.
- SLA repository. Pre-defined SLA documents of retrieved cloud services will be provided to service users. If they cannot meet the requirements of service users, tailormade SLAs will be negotiated and restored to the SLA repository.
- Transaction repository stores historical information about transactions and SLA commitments of a service provider in a given context.
- Metrics repository keeps two kinds of information: (1) metrics for system performance measurement, (2) mapping rules between low level metrics and SLA parameters for the SLA decomposition.

- Internal monitoring repository and external monitoring repository. The information of monitoring networks and resources will be stored in the internal monitoring repository for failure detections and predictions. The external monitoring repository is designed for the storage of monitoring reports that will be presented to service users, combined with solutions for potential SLA violations which are pre-defined and will be updated dynamically.

Stage 2. Service selection. To select qualified services for service users, three sub-modules collaborate with each other: (a) service retrieval module, (b) risk assessment module, and (c) service ranking module.

- Service retrieval module is used to retrieve cloud service information published on the internet according to the requirements of service users (step 1). At first, cloud service information will be discovered, retrieved and classified regularly by a semantic crawler. Then the classified information will be conceptualized by a generic Service Description Entity (SDE) metadata schema and stored in a service knowledge base that is updated consistently. Service users can search services from the service knowledge base by SPARQL query language or by interacting with the search engine using natural language. Finally, the searched services will be ranked on the basis of the level of similarities between user requirements and service descriptions (step 2).
- Risk assessment module is capable of analyzing transactional risks for service users dealing with a service provider. This purpose will be achieved by assessing the capabilities of the adherence to tailor-made SLAs of service providers. Three key sub-stages are included in designing this module. At first, the SLOs in the formed SLA (step 3, 4) will be analyzed to identify the uncertainties that will produce a negative outcome; this is the risk identification stage (step 5). The key task is to identify the business process required for SLA commitments, classify the SLOs according to their level of dependence on the service provider (dependent or non-dependent) and analyse the level of interdependency between them(common mode or independent). Specifically, network conditions and service user's situations (e.g. the robustness of customer system running on the cloud platform) are types of non-dependent events. Another key factor that should be considered in a cloud environment is the type of service provider categorized as either resource providers or brokers. When using services provided by a broker, it is necessary to take into account the risks of SLA commitments of service providers supporting the broker. At the risk assessment stage (step 6), the identified uncertain events will be analysed to determine their probability and severity of occurrence for the duration of the SLA. Two key issues will be addressed in this stage: (1) determining the probability of SLA violations. Bayesian theory will be applied to predict the incapacity of service providers committing to dependent SLOs. Based on substantial evidence (e.g. historical transaction cases or advices from other service users), the uncertainty of SLO commitments by providers (i.e. prior-probability distribution) will be decreased (i.e. posterior-probability distribution). As to the non-dependent SLOs, it is extremely difficult to have a distribution that models their occurrence trend which is spontaneous and dynamic with no certain patterns. In order to capture them, the Monte Carlo method that is suitable for learning complex and nonlinear models with uncertain parameters is regarded as one of the solutions for this problem. Other techniques that can be utilized for the analysis of non-dependent events will also be studied in this work. Additionally, the dynamic nature of transactions is one of the most significant characteristics of transactional risks, especially in cloud service provisions. Dynamic Bayesian Networks (DBNs) that are capable of modelling dynamic systems will be designed to capture such dynamicity. Meanwhile, filtering and prediction algorithms of DBN inference will be discussed. (2) Determining the financial consequences (termed the financial risks) to the service user if the SLOs have not been met as promised. The levels of transactional risks can then be identified based on the performance and financial risks analysed above. At the risk evaluation stage (step 7), a fuzzy inference model will be developed to capture the risk attitude of a user, evaluate the transactional risks to identify the threats, and assist in decision-making.
- Service-ranking module. The evaluation results will be the input of the service-ranking module (step 8) by which services provided by the service retrieval module will be ranked (step 9) by taking into account both service functions and transactional risks. Utility functions that are able to measure the interactions of several factors will be defined and services with highest utilities will be selected (step 10).

Stage 3. SLA monitoring. The tailor-made SLA of the selected service will be monitored by the SLA monitor module11. Monitoring reports and proactive solutions of potential failures of SLA violations will be presented to service users to assist them in avoiding or minimizing loss due to SLA violations. There

are seven sub-modules in the SLA monitor: SLA mapping and configuring module, network monitor, resource monitor, network analyzer, resource analyzer, SLA analyzer, and report module. Each of them is described as follows:

- SLA mapping and configuring module realize the mapping between business-level SLOs and infrastructure level KPIs, and configure monitoring parameters accordingly (step 11). Mapping rules are predefined and stored in a metrics repository. A configuration mechanism is devised to automatically configure monitors based on the decomposed SLAs and resource metrics.
- A network monitor will collect the information about networks from both service provider and service user sides (step 12).
- The monitored information will be analyzed by the network analyzer, whereby network statuses will be measured and predicted (step 13). Chaos theory and neural network technique will be used to model network traffic, and detect and predict DoS attack.
- A resource monitor, deployed on the side of service providers, is used to monitor the performance of the provisioned resources (step 12). The Ganglia Gmond module (Ganglia) will be used to monitor system performances.
- Resource-monitoring information will be analyzed by the resource analyzer from two aspects: i) checking the adherence of system performances to resource metrics and ii) real-time predicting system statuses and identifying potential failures in the near future by using failure prediction techniques (step 13), e.g. machine learning algorithms and time series prediction approaches, etc. These techniques, combined with the analysis of the features of cloud service provision systems, will be simulated and evaluated in this work to identify suitable methodologies for online predictions of system failures in cloud computing environments.
- Results of the network analysis and resource analysis are aggregated by an SLA analyzer based on mapping rules (step 14); as a result, SLA enforcement status and potential SLA violations can be monitored and predicted, which will be presented to service users by the report module (step 15).
- Solutions for predicted SLA violations will also be provided if necessary. Results of service consumption and feedback from service users will be stored in the transaction repository for next-time transactional risk assessment (step 16).

4 Evaluation of System

The proposed system is going to be evaluated in two steps: (1) the evaluation of the quality of the decision making; (2) the comparison between the results of the proposed and previous SLA-violation prediction algorithms. Specifically, the first step will be conducted by three sub-steps. Firstly, information about specific requirements and expectations of service users towards cloud services will be collected by questionnaires. In the second sub-step, the developed algorithms in this research will be applied to provide feedback to the service users on the performance of service providers in meeting the SLAs. The third sub-step refers to the stage after the service provision, in which the questionnaire surveys will be conducted again to get the satisfaction degrees and attitudes of service users against the use of the services. The results will be compared with the requirements and expectations that are collected before the service selections. Based on this, the accuracy and the efficiency of the transactional risk assessment and decision making will be measured according to the predefined evaluation policies. In the second step, the prediction results will be compared with those of previous SLA-violation prediction methods from two dimensions: time complexity and prediction accuracy.

5 Conclusion

In this paper, a user-oriented framework was developed to analyse the ability of SLA commitments of both service providers and service users, and ensure the profits of service users by two key steps: (1) designed a methodology of transactional risk assessment to assist in selecting qualified services; and (2) devised a SLA monitoring mechanism to monitor SLA enforcement and predict possible SLA violations over the lifetime of a service instance. In particular, the proposed approach took into account resource

performance and network status in the SLA monitoring mechanism as they both have significant effects on successful delivery of services to service users.

Overall, this paper introduces techniques that help service users to analyse the transactional risk and select capable cloud service providers. The framework of SLA monitoring will provide exact and detailed information of SLA commitments by providers for service users to help them effectively control and maintain their applications on the cloud platform. The techniques for system performance forecasting will enhance the accuracy of prediction of SLA violations in complex and dynamic systems. This paper enables service users to detect and predict SLA violations proactively by proposing techniques that determine beforehand the chances and consequences of the occurrence of SLA violations, which will help them to develop decisive strategies to minimize losses.

Acknowledgements

This paper is supported by the National Natural Science Foundation of China (Grants No. 61702274) and the Natural Science Foundation of Jiangsu Province (Grants No. BK20170958).

References

[1] L. Sun, H. Dong, F. K. Hussain, O. K. Hussain, E. Chang, Cloud service selection: state-of-the-art and future research directions, Journal of Network and Computer Applications 45(2014) 134-150.

[2] N. Huber, F. Brosig, S. Spinner, S. Kounev, M. Bahr, Model-based self-aware performance and resource management using the Descartes modeling language, IEEE Transactions on Software Engineering 43(5)(2017) 432-452.

[3] J. Son, A.V. Dastjerdi, R. Calheiros, R. Buyya, SLA-aware and energy-efficient dynamic overbooking in SDN-based cloud data centers, in: Proc. IEEE Transactions on Sustainable Computing, 2017.

[4] M. Ghamkhari, A. Wierman, H. Mohsenian-Rad, Energy portfolio optimization of data centers, in: Proc. IEEE Transactions on Smart Grid, 2017.

[5] W. Hussain, F.K. Hussain, O.K. Hussain, E. Chang, Provider-based optimized personalized viable SLA (OPV-SLA) framework to prevent SLA violation, The Computer Journal 59(12)(2016) 1760-1783.

[6] M.C. Lacity, S. Solomon, A. Yan, L.P. Willcocks, Business process outsourcing studies: a critical review and research directions, Journal of Information Technology 26(4)(2011) 221-258.

[7] K. Lu, R. Yahyapour, P. Wieder, E. Yaqub, M. Abdullah, B. Schloer, C. Kotsokalis, Fault-tolerant service level agreement lifecycle management in clouds using actor system, Future Generation Computer Systems 54(2016) 247-259.

[8] W. Hussain, F.K. Hussain, O. Hussain, E. Damiani, E. Chang, Formulating and managing viable SLAs in cloud computing from a small to medium service provider's viewpoint: a state-of-the-art review, Information Systems 71(2017) 240-259.

[9] O. Anya, H. Ludwig, M. Mohamed, S. Tata, Sla analytics for adaptive service provisioning in the cloud, in: Proc. IEEE/IFIP Network Operations and Management Symposium, 2016.

[10] G. Katsaros, T. Metsch, J. Kennedy, Slaas: an OCCI compliant framework for cloud SLA provisioning and violation detection, in: Proc. the 6th International Conference on Cloud Computing and Services Science, 2016.

[11] D. Ardagna, M. Ciavotta, M. Passacantando, Generalized Nash equilibria for the service provisioning problem in multi-cloud systems, IEEE Transactions on Services Computing 10(3)(2017) 381-395.

[12] O.K. Hussain, Z.-u. Rahman, F.K. Hussain, J. Singh, N.K. Janjua, E. Chang, A user-based early warning service management framework in cloud computing, The Computer Journal 58(3)(2015) 472-496.

[13] W.A. Michalk, C. Weinhardt, B. Blau, T. Conte, W. Michalk, L. Filipova-Neumann, B. Blau, W. Michalk, B. Blau, SLA

establishment decisions: minimizing the risk of SLA violations, Service Science 9(2011) 206-222.

[14] H. Ma, Z. Hu, K. Li, H. Zhang, Toward trustworthy cloud service selection: A time-aware approach using interval Neutrosophic set, Journal of Parallel and Distributed Computing 96(2016) 75-94.

[15] L. Wu, S.K. Garg, S. Versteeg, R. Buyya, SLA-based resource provisioning for hosted software-as-a-service applications in cloud computing environments, IEEE Transactions on Services Computing 7(3)(2014) 465-485.

[16] O. Fachrunnisa, F.K. Hussain, A methodology for maintaining trust in industrial digital ecosystems, IEEE Transactions on Industrial Electronics 60(3)(2013) 1042-1058.

[17] J. Abdullah, A. van Moorsel, Uncertainty and uncertainty tolerance in service provisioning, Journal of Internet Services and Information Security 1(4)(2011) 89-109.

[18] Y.-J. Ren, J. Shen, J. Wang, J. Han, S.-Y. Lee, Mutual verifiable provable data auditing in public cloud storage, Journal of Internet Technology 16(2)(2015) 317-323.

[19] J.-Y. Hu, C.-H. Wu, C.-C. Chu, K.-H. Liang, H.-C. Young, Y.-Y. Hsu, C.H. Hu, H.-G. Lin, Constructing a cloud-centric service assurance platform for computing as a service, in: Proc. International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, 2011.

[20] L. Romano, D. De Mari, Z. Jerzak, C. Fetzer, A novel approach to QoS monitoring in the cloud, in: Proc. First International Conference on Data Compression, Communications and Processing (CCP), 2011.

[21] B. Ciciani, D. Didona, P. Di Sanzo, R. Palmieri, S. Peluso, F. Quaglia, P. Romano, Automated workload characterization in cloud based transactional data grids, in: Proc. IEEE 26th International Parallel and Distributed Processing Symposium Workshops & PhD Forum (IPDPSW), 2012.

[22] B.D. Ripley, The r project in statistical computing, MSOR Connections. The newsletter of the LTSN Maths, Stats & OR Network 1(1)(2001) 23-25.

[23] A.C. Oliveira, H. Chagas, M. Spohn, R. Gomes, B.J. Duarte, Efficient network service level agreement monitoring for cloud computing systems, in: Proc. 2014 IEEE Symposium on Computers and Communications (ISCC), 2014.

[24] S.K. Garg, A.N. Toosi, S.K. Gopalaiyengar, R. Buyya, SLA-based virtual machine management for heterogeneous workloads in a cloud datacenter, Journal of Network and Computer Applications 45(Suppl. C)(2014) 108-120.

[25] D. Serrano, S. Bouchenak, Y. Kouki, F.A. de Oliveira Jr, T. Ledoux, J. Lejeune, J. Sopena, L. Arantes, P. Sens, SLA guarantees for cloud services, Future Generation Computer Systems 54(2016) 233-246.

[26] A.A.Z.A. Ibrahim, D. Kliazovich, P. Bouvry, Service level agreement assurance between cloud services providers and cloud customers, in: Proc. 2016 16th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGrid), 2016.

[27] G. Liu, H. Shen, H. Wang, Deadline guaranteed service for multitenant cloud storage, IEEE Transactions on Parallel and Distributed Systems 27(10)(2016) 2851-2865.