Journal of Computers Vol. 30 No. 1, 2019, pp. 23-30
doi:10.3966/199115992019023001003

Survey of Cloud SLA Assurance in Pre-interaction and Post-interaction Start Time Phases

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

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

[2] Centre for Applied Informatics, 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. Service level agreements (SLAs) are contracts that define the responsibilities, rights and charging policies of cloud service providers and users, in terms of the functional and non-functional requirements (e.g. QoS performance) of service users. In a cloud provisioning process, service providers and users use SLAs as rules that the provisioned services should comply with to maximize profits of both sides. In this paper, we review the state-of-the-art of SLA assurance in Cloud computing, identify gaps in existing SLA assurance research, and summarise key research issues.

Keywords: cloud service, literature review, SLA assurance

1 Introduction

Nowadays, cloud computing resources are normally delivered in the form of complex services. Cloud services are deployed and provisioned in three common architectures: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).

Service level agreements (SLAs) are contracts that define the responsibilities, rights and charging policies of cloud service providers and users, in terms of the functional and non-functional requirements (e.g. QoS performance) of service users. A cloud SLA formally contains the following elements [1]: key performance indicators (KPIs, e.g. availability, reliability and response time) that need to be guaranteed by service providers over a stimulated time period; time periods in which KPI guarantees are ensured; the granularity of guaranteed services, i.e. the resource scales the KPIs are measured with; factors that are excluded from the guaranteed KPIs; credits of service users or penalties of non-guaranteed KPIs; and monitoring, measurement and reporting of KPI violations.

In a cloud provisioning process, service providers and users use SLAs as rules that the provisioned services should comply with to maximize profits of both sides. A Forrester Consulting survey report [2] states that service providers meet the expected outcomes only 74% of the time. In addition, reports in the literature mentions that 91% of unhappy customers of a provider will never use the services again, and will give a negative impression of the service provider to the existing or potential customers. Meanwhile, a 5% of reduction in customer defection rate can improve profits by 25%-100% [3].

In this paper, we review the state-of-the-art of SLA assurance in Cloud computing, identify gaps in the existing SLA assurance research, and summarise key research issues in this area. We survey the SLA assurance techniques based on the time periods of service transaction and provision: SLA assurance in pre-interaction-start time phase and in post-interaction-start time phase [2]. In pre-interaction-start time phase, the literature is analysed from the viewpoints of service providers and service users respectively.

[*] Corresponding Author

In post-interaction-start time phase, the literature is categorised based on four aspects: performance monitoring and SLA assurance; security term consideration and monitoring in SLAs; SLA assurance based on trust evaluation; and trade-offs between energy consumption and performance maximization. This literature review is a follow-up of our previous work [2], which covers the SLA assurance research done in recent five years (20132017), and does a more comprehensive review and technique comparison compared with [2].

We summarise four key research issues based on the reviewed literature: lack an effective tool of risk assessment and evaluation for cloud service selection in the pre-interaction-start time phase; lack an approach for service users making informed decisions for the selection of capable service providers with minimum risks of SLA violations and maximum similarities of functions required by service users; lack a SLA monitoring framework for service users automatically obtaining detailed information about resource consumption during the process of cloud service delivery; and lack tools to detect and predict SLA violations in the complex and dynamic cloud environment.

The structure of this paper is as: section 2 reviews the state-of-the-art work of SLA assurance in cloud, and identifies research gaps in the existing literature; section 3 summarises the key research issues; section 4 concludes this paper.

2 State-of-The-Art of SLA Assurance

In this section, the literature pertaining to the area of SLA assurance is explored from two aspects: (1) Risk assessment in Pre-interaction-start Time Phase; and (2) performance monitoring and forecasting in Post-interaction-start Time Phase. The state-of-the-art in this area is presented and discussed and the research gaps are identified. At last, we present the key research issues in these two areas to highlight the challenges that need to be addressed in the near future.

2.1 Risk Assessment in Pre-interaction-start Time Phase

The background and related work in this section falls within two areas: (1) SLA-based risk assessment from the perspective of service provider; (2) SLA-based risk assessment from service users' perspective; (3) Gaps in transactional risk assessment in pre-interaction-start time phase.

SLA-based risk assessment from the perspective of service provider. Various approaches were proposed for service provisioning decisions of service providers when establishing SLAs [4-5]. Anya et al. [6] 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. [7] 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. [8] 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. [9] 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 ensure the requirements of service providers and service users, and to proactively assure SLAs, Hussain et al. [10] further proposed a profile-based SLA violation prediction model that starts monitoring SLAs before the deployment and the running of the service. The proposed method predicts the possible resource usage of service users based on their reputation that is formed by analysing the service users' historical transactions, which helps service providers make decisions of SLA establishment and assurance.

An efficient establishment of cloud SLAs would improve the service running performance and ease the business transaction process. Hussain et al. [11] designed an architecture for SLA establishment, which supports service providers taking into account the reliability and trustworthiness of service users. The proposed resource allocation framework helps service providers make decisions on resource allocation based on the service user's reliability defined in the SLA. To support the automatic SLA management in cloud computing, a cloud SLA template, called CSLAT, was proposed by [12], which formally defined the decisive parameters for cloud service deployment and running. These definitions prevent parameter conflicts and uncertainties in SLAs. García et al. [13] introduced a SLA-aware PaaS Cloud platform, namely Cloudcompaas, to manage cloud resource lifecycle. The Cloudcompaas extends the WSAgreement to specify the features of cloud services. It establishes a mechanism to adaptively correct the QoS violations based on the elasticity of IaaSs.

SLA-based risk assessment from the perspective of service users. Existing research is dedicated to the uncertainty of consumers' 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.

Along with the spread of the cloud outsourcing and cloud federation, the trust levels of cloud providers are becoming an important factor for consumers selecting informed cloud services. Moyano et al. [18] introduced a trust evaluation method for service users identifying the trustworthiness of service providers. The proposed trust model uses a trust interval technique to capture uncertainness during the evaluation process. And this trust evaluation method was applied to solve e-health problems. Mourougan et al. [19] developed a regression tree based trust evaluation model to evaluate trusts of different cloud service providers and to help federate different kinds of services. The method aggregates policy-based trust, reputation trust, evidence-based trust and SLA verification trust to build federated cloud services that guarantee expected security and privacy levels. Fu et al. [20] proposed a searchable encryption scheme to protect cloud data privacy before the data is outsourced. The proposed method supports parallel and multi-keyword search. Xia et al. [21] also focused on solving problems of sensitive data outsourcing. Especially, their method can support the dynamic operations, such as the deletion and insertion operations simultaneously.

Gaps in transactional risk assessment in pre-interaction-start time phase. In the above discussion, three issues of transactional risk assessment in previous work are emphasized as follows: (1) Most of the work was proposed for service providers, helping them manage multiple SLAs to avoid future SLA violations, while investigation of transactional risks is of paramount importance for service users as well. (2) Little work has been carried out for transactional risk assessment in cloud service selection. Current work more focuses on Grid or Web service selection, whereas cloud services with different features such as on-demand self-service and rapid elasticity should be given new consideration. (3) Existing techniques for transactional risk assessment neither focus on interactions of multiple transaction agents, nor consider the influences of former decisions on subsequent actions.

2.2 SLA Monitoring and Forecasting in Post-interaction-start Time Phase

SLA monitoring strategies as well as detection and prediction of possible SLA violations were actively studied and developed in service-based environments. In this section, we compare and summarise recent works on service monitoring systems from four aspects: (1) Performance monitoring and SLA assurance; (2) Security term construction in SLAs; (3) SLA assurance based on trust evaluation; and (4) Trade-offs between energy consumption and performance maximization.

Performance monitoring and SLA assurance. Chu et al. [22] proposed a model to support the design and construction of enterprise cloud services on different types of cloud platforms. The model can also monitor and analyse QoS performance in real-time to prevent SLA violation during service runtime. Ait-Idir et al. [23] introduced a QoS monitoring and assurance approach based on the procedure of SLA enforcement of scheduled applications to guarantee the expected QoS performance during service provisioning. Maarouf et al. [24] developed a framework of QoS monitoring and satisfaction of users' QoS requirements by guaranteeing the implementation of terms in SLAs. This work uses a third-party service provider to monitor the QoS and to ensure the service performance and reliability. Khan et al. [25] proposed a QoS monitoring framework and defined performance measuring metrices to adaptively guarantee QoS performance. Remedy actions are defined in the framework to rectify SLA violations during runtime. Monetary penalization would be taken as long as non-compliance to SLAs occurs. Cedillo et al. [26] proposed a real-time monitoring process that specifies non-functional performance metrics in SLAs. The reflection mechanisms of the monitoring procedure supports high flexibility and adaptability. The requirement changes enable the changes of the monitoring infrastructure. The monitoring procedure interacts with cloud services during runtime, collects and analyses performance data, and reports issues of non-compliance to SLAs. Zhao et al. [27] proposed a SLA management framework for cloud databases. The proposed framework adaptively and dynamically provision data storage resources for cloud applications by ensuring the SLA performance satisfaction of users' requirements. The framework monitors the SLAs of applications during runtime, and triggers corrective actions of SLA violation to avoid monetary costs.

Security term construction and monitoring in SLAs. Avoiding the risk of Cloud security is one of the most important factor for assuring SLAs. To manage service security during run time. Kaaniche et al. [28] proposed an extension of rSLA (a SLA describing language), namely sec-rSLA, to enable rSLA describe security requirements from the perspective of service providers. The authors also integrated a mechanism to rSLA to support the management and enforcement of the security SLA. The sec-rSLA presents an overview of security requirements of service users and support the discovery of the most appropriate tools to monitor the required security levels in real time. The combination of heterogeneous clouds and the lack of a standard security measures on cloud services lead to the difficulty of cloud deployment and delivery. Rios et al. [29] introduced a method of monitoring the service security based on the development and the runtime assurance of SLA metrices. The service monitoring scheme is deployed by the Mont image Monitoring Tool, and based on data mining techniques to implement online monitoring and analysis of performances of both applications and networks. Teshome et al. [30] defined security monitoring terms in cloud SLAs. The authors designed a security monitoring strategy that incrementally constructs SLA terms and verifies the SLA assurance.

In the work of [31], THEMIS, a secure and non-obstructive billing system, was proposed to overcome the limitation of current billing systems in terms of security capabilities or computational overhead. In this system, an SLA monitoring module, called S-Mon, was devised to enhance its security capability. Two noteworthy aspects of this monitoring module are: firstly, the monitoring report would be presented to users only after one service session is finished or when the user requires the monitoring data. Secondly, details about system status are detected. However, this paper neither discussed how these data can be mapped to SLA parameters, nor considered the prediction of SLA violations. To monitor security performance for SLA-based cloud services, Petcu et al. [32] present the definitions, mechanisms and tools of measuring and monitoring securities. The authors also discussed the barriers in the existing work.

SLA assurance based on trust evaluation. The work of [33] studied the problems of cloud resource management and placement based on SLA assurance. The authors defined quantitative and normalized metrics of availability, response time, and trustworthiness, and used non-linear optimization model to formalize and address the resource management problems. Cicotti et al. [34] stated that a reliable QoS monitoring device would improve the trust worthiness of agents in cloud service provisions and consumptions. Therefore, they designed a QoS monitoring facility, namely QoSMONaaS, to consistently virtualize cloud users in "X as a service" contexts based on the analysis of SLAs. Jules et al. [35] proposed that in a cloud service provisioning process, a service provider normally optimizes resource allocations without knowing the service consumers' behaviour, which can lead to SLA violations. Therefore, the authors designed a service selection framework that selects service providers based on their trust evaluation. They also present a dynamic SLA construction and maintaining scheme based on the probabilistic ontology techniques to dynamically detect SLA violations.

Trade-offs between energy consumption and performance maximization. One challenge of cloud service provisioning is to balance the trade-off between power consumption and service performance. As the proliferation of cloud services, energy and power consumption is increasing. Hurson et al. [36] illustrated a practical SLA-based resource management case to analyse how the state-of-the-art resource scheduling algorithms improve energy consumption efficiencies. To balance energy saving and SLA assurance, Glasser et al. [37] proposed a VM migration approach that runs VMs on more physical hosts to ensure SLA requirements, compared with the previous power minimizing algorithms. Validation shows that the proposed approach achieves a better trade-off between energy consumption and SLA performance assurance. Singh et al. [38] pointed out that an efficient way of resource scheduling can help to reduce energy consumption by cloud services. The authors implemented a number of algorithms to study and analyse the influence of different parameters on scheduling performance of cloud resources. Effective VM consolidation reduces power consumption during service provisioning. Motwani et al. [39] proposed an SLA and Energy Aware policy for real-time VM consolidations in Cloud data centres to optimize the power and guarantee the service performance. Ciciani et al. [40] 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. WA allows the prediction of SLA violation and enables service users to have full control over what they want to be notified about.

Gaps in SLA monitoring and forecasting in post-interaction-start time phase. We discuss the identified gaps of SLA Monitoring and Forecasting in Post-interaction-start Time Phase.

Service user-oriented. The use of SLAs is one of the possible ways to overcome the challenge of providing a means of service quality control to service users. Some of the work establishes user-friendly visiting mechanisms that assist service users to conveniently interact with the monitoring system. However, these systems are designed from the providers' perspective. They cannot present SLA-level monitoring information consistently and provide informed opinion to users when necessary.

SLA decomposition. SLA decomposition is used to map low level system performance metrics to high level SLA parameters. Most of the work assumes that the SLA monitor mainly serves the needs of service providers, while mapping rules for users are different from those for providers because apart from resource performance, interaction capabilities between service providers and service users (e.g. network conditions) should also be considered when referring to the measurement of users' satisfaction.

Intervals of measurement. Some work focuses on the identification of measuring intervals. Although progress has been made in this area, the determination of measuring intervals in cloud paradigms is far from trivial, especially when comes to user-oriented environments.

Prediction of SLA violations. Based on the discussion in literature review, currently the most popular methodology for SLA violation prediction is using threat thresholds to detect the potential occurrence of SLA violations. However, several issues should be resolved in such situation, for example: (1) what is the probability of real SLA violation when a threshold is violated? (2) What is the loss of system adaptation if a fallacious threshold violation is detected? One of the key objectives of this work is to explore prediction algorithms for SLA violations in cloud paradigms, providing informed information of SLA enforcement for service users.

3 Identified Key Research issues in Sla Assurance

An analysis of the existing approaches in the literature reveals that there have been many achievements in terms of SLA assurance in cloud computing. However, few studies have paid any attention to examining the complexity and unpredictability of cloud systems and the obstacles that arise from them in making informed decisions and establishing tailor-made SLAs. Therefore, the identified research issues are as follows:

- Lack an effective tool of risk assessment and evaluation for cloud service selection in the pre-interaction-start time phase.
- Lack an approach for service users making informed decisions for the selection of capable service providers with minimum risks of SLA violations and maximum similarities of functions required by service users
- Lack a SLA monitoring framework for service users automatically obtaining detailed information about resource consumption during the process of cloud service delivery
- Lack tools to detect and predict SLA violations in the complex and dynamic cloud environment that will help service users minimize the losses experienced by SLA violations

4 Conclusion

In this paper, we did a comprehensive survey on SLA assurance in cloud computing, identified gaps in the existing SLA assurance research, and summarized key research issues in this area. We reviewed the SLA assurance work in two times periods: SLA assurance in pre-interaction-start time phase and in post-interaction-start time phase. In pre-interaction-start time phase, the literature was analyzed from the viewpoints of service providers and service users respectively. In post-interaction-start time phase, the literature was categorized in terms of four aspects: performance monitoring and SLA assurance; security term consideration and monitoring in SLAs; SLA assurance based on trust evaluation; and trade-offs between energy consumption and performance maximization. The identified research issues gave future research directions on SLA assurance of cloud services.

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] S.A. Baset, Cloud SLAs: present and future, ACM SIGOPS Operating Systems Review 46(2)(2012) 57-66.

[2] L. Sun, J. Singh, O.K. Hussain, Service level agreement (SLA) assurance for cloud services: a survey from a transactional risk perspective, in: Proc. the 10th International Conference on Advances in Mobile Computing & Multimedia, 2012.

[3] B.E. Hosmer, The loyalty effect: the hidden force behind growth, profits, and lasting value, Consulting to Management 10(2)(1998) 82.

[4] 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.

[5] 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.

[6] O. Anya, H. Ludwig, M. Mohamed, S. Tata, SLA analytics for adaptive service provisioning in the cloud, in: IEEE/IFIP Network Operations and Management Symposium, IEEE Xplore, 2016, pp. 1093-1096.

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

[8] 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.

[9] 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.

[10] W. Hussain, F.K. Hussain, O. Hussain, E. Chang, Profile-based viable service level agreement (SLA) violation prediction model in the cloud, in: Proc. 2015 10th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), 2015.

[11] 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.

[12] D. Rane, M. Sarma, CSLAT: an SLA template for cloud service management, International Journal of Communication Networks and Distributed Systems 14(1)(2014) 19-39.

[13] A.G. García, I.B. Espert, V.H. García, SLA-driven dynamic cloud resource management, Future Generation Computer Systems 31(2014) 1-11.

[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] F. Moyano, K. Beckers, C. Fernandez-Gago, Trust-aware decision making methodology for cloud sourcing, in: Proc. International Conference on Advanced Information Systems Engineering, 2014.

[19] S. Mourougan, M. Aramudhan, Regression tree based ranking model in federated cloud, Indian Journal of Science and Technology 9(22)(2016).

[20] Z. Fu, X. Sun, Q. Liu, L. Zhou, J. Shu, Achieving efficient cloud search services: multi-keyword ranked search over encrypted cloud data supporting parallel computing, IEICE Transactions on Communications E98.B(1)(2015) 190-200.

[21] Z. Xia, X. Wang, X. Sun, Q. Wang, A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data, IEEE Transactions on Parallel and Distributed Systems 27(2)(2016) 340-352.

[22] W.C.C. Chu, C.T. Yang, C.W. Lu, C.H. Chang, N.L. Hsueh, T.C. Hsu, S. Hung, An approach of quality of service assurance for enterprise cloud computing (QoSAECC), in: Proc. 2014 International Conference on Trustworthy Systems and Their Applications, 2014.

[23] M. Ait-Idir, N. Agoulmine, Enhancing cloud capabilities for SLA enforcement of cloud scheduled applications, in: Proc. 2016 IEEE/ACM 9th International Conference on Utility and Cloud Computing (UCC), 2016.

[24] A. Maarouf, A. Marzouk, A. Haqiq, Automatic control of the quality of service contract by a third party in the cloud computing, in: Proc. 2014 Second World Conference on Complex Systems (WCCS), 2014.

[25] H.M. Khan, G.-Y. Chan, F.-F. Chua, An adaptive monitoring framework for ensuring accountability and quality of services in cloud computing, in: Proc. 2016 International Conference on Information Networking (ICOIN), 2016.

[26] P. Cedillo, J. Jimenez-Gomez, S. Abrahao, E. Insfran, Towards a monitoring middleware for cloud services, in: Proc. 2015 IEEE International Conference on Services Computing, 2015.

[27] L. Zhao, S. Sakr, A. Liu, A framework for consumer-centric SLA management of cloud-hosted databases, IEEE Transactions on Services Computing 8(4)(2015) 534-549.

[28] N. Kaaniche, M. Mohamed, M. Laurent, H. Ludwig, Security SLA based monitoring in clouds, in: Proc. IEEE International Conference on Edge Computing (EDGE), 2017.

[29] E. Rios, W. Mallouli, M. Rak, V. Casola, A.M. Ortiz, SLA-driven monitoring of multi-cloud application components using the Musa framework, in: Proc. IEEE 36th International Conference on Distributed Computing Systems Workshops (ICDCSW), 2016.

[30] A. Teshome, L. Rilling, C. Morin, Verification for security monitoring SLAs in IaaS clouds: the example of a network ids, [Ph.D. dissertation], Inria Rennes Bretagne Atlantique, 2017.

[31] K.-W. Park, J. Han, J. Chung, K.H. Park, Themis: a mutually verifiable billing system for the cloud computing environment, IEEE Transactions on Services Computing 6(3)(2013) 300-313.

[32] D. Petcu, C. Craciun, Towards a security SLA-based cloud monitoring service, in: Proc. International Conference on Cloud Computing and Services Science, 2014.

[33] K. Xiong, X. Chen, Ensuring cloud service guarantees via service level agreement (SLA)-based resource allocation, in: Proc. 2015 IEEE 35th International Conference on Distributed Computing Systems Workshops, 2015.

[34] G. Cicotti, L. Coppolino, S. D'Antonio, L. Romano, How to monitor QoS in cloud infrastructures: the QoSmonaas approach, International Journal of Computational Science and Engineering 11(1)(2015) 29-45.

[35] O. Jules, A. Hafid, M.A. Serhani, Bayesian network, and probabilistic ontology driven trust model for SLA management of cloud services, in: Proc. IEEE 3rd International Conference on Cloud Networking (CloudNet), 2014.

[36] A.M. Sampaio, J.G. Barbosa, Chapter three - energy-efficient and SLA-based resource management in cloud data centers, Advances in Computers 100(Suppl. C)(2016) 103-159.

[37] P.M. Glasser, O. Kocabas, B. Kantarci, T. Soyata, J. Matthews, Energy efficient VM migration revisited: SLA assurance and minimum service disruption with available hosts, in: Proc. International Conference on High-Capacity Optical Networks and Enabling/Emerging Technologies (HONET), 2015.

[38] H. Singh, S. Tyagi, P. Kumar, Energy-conscious resource scheduling in cloud computing environment: a pragmatic view, in: Proc. 2016 2nd International Conference on Next Generation Computing Technologies (NGCT), 2016.

[39] A. Motwani, V. Patel, V.M. Patil, Power and QoS aware virtual machine consolidation in green cloud data center, International Journal of Electrical, Electronics and Computer Engineering 4(1)(2015) 93.

[40] 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.