A Common Reference Model for Cloud Services Customer Agreements*

José María García[1,2], Octavio Martín-Díaz[2], Carlos Müller[2], Pablo Fernández[1,2], and Antonio Ruiz-Cortés[1,2]

[1] Smart Computer Systems Research and Engineering Lab (SCORE)
[2] Research Institute of Informatics Engineering (I3US)
Universidad de Sevilla, Spain
{josemgarcia,omartindiaz,cmuller,pablofm,aruiz}@us.es

Abstract. Services in cloud computing are always used under the legal terms defined in their customer agreements. Providers have to specify their terms considering applicable jurisdictions, using varying terminologies that make their compliance checking and analysis operations difficult to generalize and automate. In this paper, we present a reference model as a first step towards obtaining a common specification that will facilitate the operationalization of customer agreement's terms of service, while enabling the alignment of the different terminologies used by service providers.

Keywords: Customer Agreements · Service-Level Agreements · Regulatory Compliance · Automated Analysis.

1 Introduction

There are many existing works on legal aspects of cloud-related contracts, commonly known as service agreements or more generically customer agreements (CA), which not only include the corresponding service level agreement (SLA), but also the terms of service, the privacy policy and the acceptable user policy, among other elements [2, 4, 8, 11]. However, these approaches present differences in terminology and country-related regulations that in turn prevent providers to agree on a common model as foundations for their CAs. Furthermore, CA enforceability and legal claims depend on the jurisdictions and/or regulations that are applicable, thus making the compliance and other analysis operations over CAs much more challenging [3, 5–8, 13].

Automated analysis of CAs have been traditionally focused on SLAs, where the service level objectives play a fundamental role when monitoring the compliance with SLAs and obtaining corresponding compensations [12]. There are also

* This work has been partially supported by the European Commission (FEDER) and Junta de Andalucia under projects APOLO (US-1264651) and EKIPMENT-PLUS (P18-FR-2895), by the Spanish Government (FEDER/Ministerio de Ciencia e Innovación – Agencia Estatal de Investigación) under project HORATIO (RTI2018-101204-B-C21)

recent efforts that propose analysis operations for pricing and billing terms [9], but less approaches try to operationalize other elements of CAs, such as the terms of service, or the privacy policies, to name a few. In this initial work, we approach these challenges by devising a common reference model to specify CAs that will support the such operationalization of their different parts. We have analyzed various sources to design our proposed model, while allowing the mapping between our model and the terminology used in cloud service providers' CAs.

The remaining of this paper is organised as follows. Section 2 presents the reference model we have elaborated that provides a common terminology to analyse CAs. Next, Section 3 discusses the operationalization of some of the CA elements discussed before. Next, Section 4 reviews the related work. Finally, Section 5 presents our conclusions and future work.

2 Reference Model

Bradshaw et al., lawyers from the Universities of London and Oxford, provide in [8] a comparison between several well known cloud providers contracts and they analyze their compliance to US and EU regulations. In turn, Graux, Ypma et al., present the final report for the European Commission about standards regarding with SLAs for the Cloud comparing the regulations from EU countries [11]. Such a work has differences from the glossary in [8]; as an example, in this report "*Service Quality Assurance*" refers to some aspects of the privacy policy exposed in [8]. In addition, the National Institute of Standards and Tecnhnology (NIST) of the US government establishes in [4] some guidelines and recommendations for assessing security and privacy policies in the cloud computing adoption and they mostly uses the glossary proposed in [8]. We have analysed the commonality in these sources to get our proposed reference model for customer agreements that is exposed in the following sections.

2.1 Customer Agreements

In the literature and cloud providers documents, "service agreements" and "customer agreements" (CA) can be both commonly found as synonym describing a binding between providers and customers. From a legal perspective the key is considering such a binding as a "contract", thus enforceable in law courts. Therefore, as depicted in Figure 1, we use "contract" as a pivotal element of our proposed CA reference model.

A "contract" is characterized by the service provider, the provided service, a duration, and a target audience.

A "service provider" may offer either a unique contract for all services (e.g. Microsoft Azure exposes the same customer agreement for all their provided services), or a different contract for each provided service (e.g. Google). In the Cloud context, the nature of a service is mostly Infrastructure as a Service (IaaS), Platform as a Service (PaaS), or Software as a Service (SaaS).

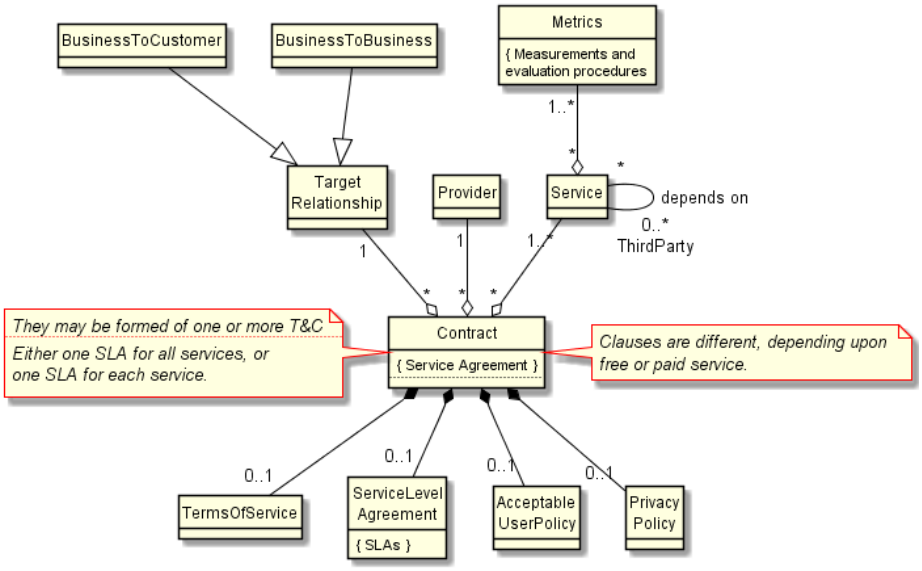

Fig. 1. Model for customer agreements.

Although a "service" can be freely offered by a provider, the CA constitutes an enforceable contract for paid services and their contents may differ depending on such a purpose from now on.

Provided services are related to several metrics that must be measured and evaluated in a monitoring process [14]. The monitoring result can be used with different purposes, as explained later in this paper.

The contract may refer, as target audience, to either "Business to Customer" (B2C) or "Business to Business" (B2B) relationships. Businesses span from small and medium enterprises, corporations, and administrations. They all may have different perspectives from a legal viewpoint.

Providers may require their customers to accomplish certain conditions, in order to avoid illegal or controversial activities they are not willing to host. Thus, it is commonly described an "Acceptable User Policy" which includes terms regarding with applications critical to human safety, mass destruction weapons, nationals from some countries, unacceptable behavior, etc.

Additionally, contracts are mostly composed of the service-level agreement (SLA), terms of service (TS), and the privacy policy (PP). Each of them are explained in the following sections.

2.2 Service-Level Agrements

Service level Agreements and their related elements depicted in Figure 2 are essential elements in CAs for paid services. They are comprised of "Service-Level Objectives" (SLOs).

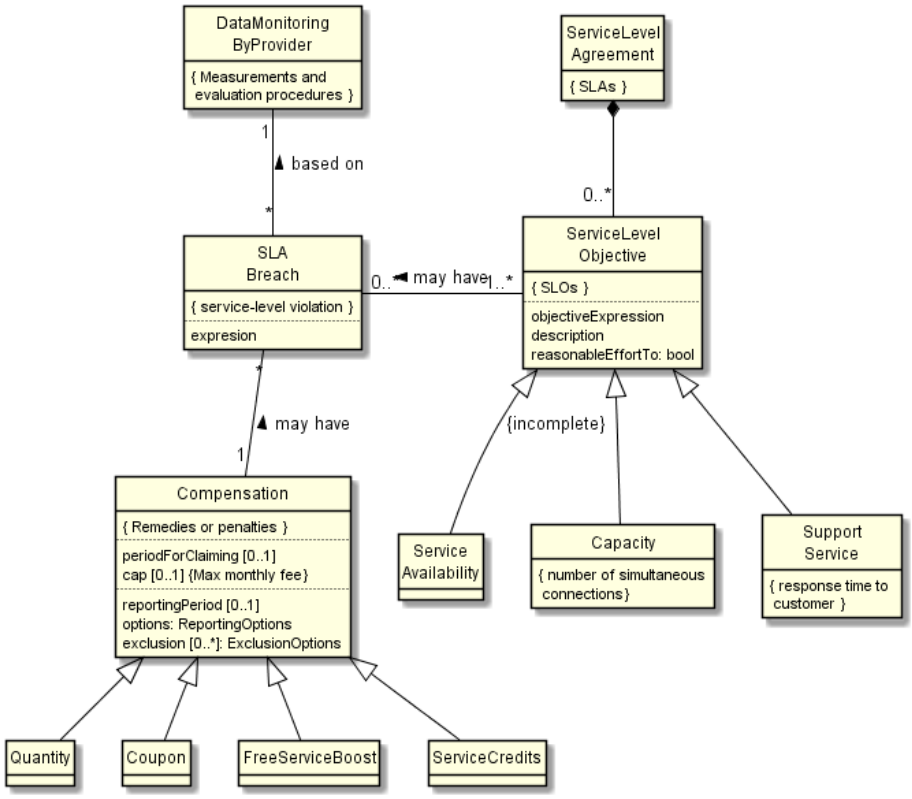

Fig. 2. Model for service-level agreements.

SLOs are obligations which implies a legal binding between agreement participants, from providers to customers. They are usually specified as conditions based on one or more metrics involved in the service provisioning. Among others, these metrics are the service availability, the capacity in terms of number of simultaneous connections for a period, and the response time to incidences reported to the customer support service. In some cases, specially in free service provisions, SLOs are expressed in terms of a "*reasonable effort to*", for customers to be aware that such obligations cannot be claimed to providers at any circumstance. However, there are some providers that make use of these kind of ambiguous expressions even in case of non-free services, as can be seen in Amazon AWS or Microsoft.

SLOs fulfillment must be monitored at service provisioning time in order to check the SLA compliance. There are several measurements and evaluation procedures which result in log files containing the data monitored by providers. Both measurements and metrics are SLA constituents [14]. However, it is usually hard for customers to obtain in a precise way the actual performance offered

by their providers and thus, they may use third-party solutions to tackle this problem.

Based on monitored data, SLOs can be proved to be not fulfilled, incurring in "SLA Breach" (a.k.a. service level violation). In these cases, one or more "compensations" [12] (a.k.a remedies or penalties) apply[3]. These compensations can be defined by means of bill discounts, service credits to be returned in further service provision, or coupons. They are mostly computed in a monthly basis, and can be limited with a maximum quantity, usually the monthly price or equivalent. In addition, there is a period for customers to claim their compensation, and accordingly, a period for providers to report the log files in case of breach.

There are also exclusions by which providers declare compensations not to be applicable, such as network failures or configuration errors due to customer's software, violations of acceptable user policies, beta or trial services, and scheduled maintenance.

2.3 Terms of Service

As SLAs describe the service levels offered when a service is being provided, "Terms of Service" (TS) regulate the provided services themselves. Thus, as depicted in Figure 3 they comprise aspects such as liability, pricing plans, variations, proprietary rights, warranties, jurisdiction, and indemnification.

"Liability" refers to provider's disclaimers or, in other words, limitations to provider's responsibility because of force-majeure events in which they will not indemnify their customers. Some examples are: wars or civil disturbances, terrorism, epidemic or natural disasters, cyber-atacks against infrastructures, and so-called "*acts of God*" for unforeseeable or unavoidable events. Liability may be either direct or indirect. Direct liability refers to exclusions for damages or losses to customers, even for services which were contracted in some cases. EU jurisdiction is much more protective than US in such cases. In turn, indirect liability refers to disclaimers against potential large scale damages, and can be very controversial in case of disputes. In addition, limits to liability can be described to avoid high indemnifications (which can be controversial if denying any kind of liability) and can be related to location. Other exceptions to liability may imply services interruptions in provider's datacenters due to third parties, or local incidents due to provider's personnel.

Different "pricing plans" [1, 10] can be described for services. Some variants are: (1) pay-per-usage when customers use services on demand; (2) reservation when customers reserve the use of a service in exchange of a reduced pay-per-usage; (3) volume-price when the customers make an unique, monthly payment for using several services; or (4) one-payment when the customers make an unique, yearly payment for using several services. Except for the former, the remaining plans include some kind of discounts to be applied. Billing [9] is usually given in a monthly basis, be at the beginning of the month, otherwise a fixed day during the month.

[3] There are also contracts in which customers pay a reward to providers in case of SLAs over-fulfillment.

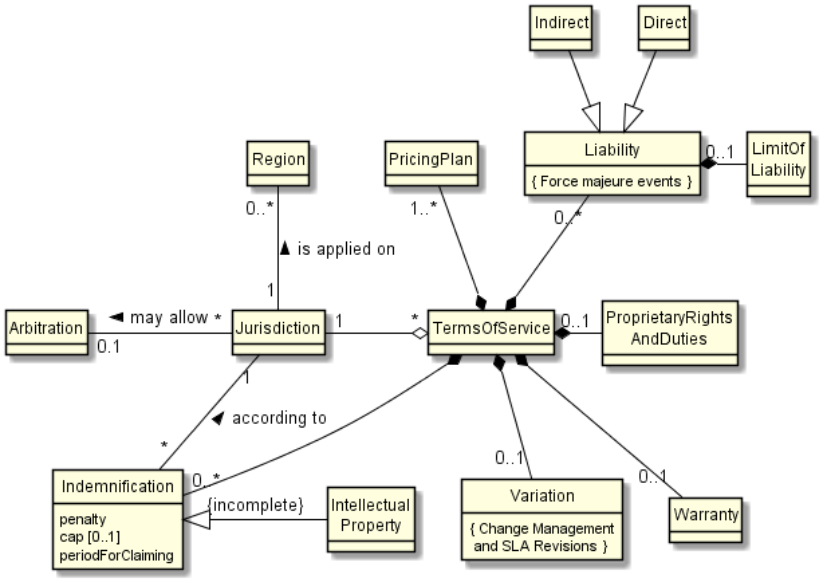

Fig. 3. Model for terms of service.

"Variation" refers to SLA revisions and change management. It usually goes from warnings on change, remainders of the provider's right to change, or breaking clauses for customers to withdraw. Customers should have (1) access to previous TS versions in order to accept or reject a new TS version, (2) implicit acceptation on using, or (3) right to terminate instead.

In terms of "proprietary rights and duties", providers do not usually claim rights over customer data or intellectual properties, retaining only rights over their own services. Customers may grant license for republishing their data for a proper service provision, but with a possible abusive coverage. This issue might be even not addressed at all.

Regarding "warranties", most usually the SLA which is linked to the TS is the only warranty, though the EU regulations are much more protective in this topic.

The "jurisdiction" concerns the region where provider's datacenters are physically placed. As just said above, EU regulations are much more protective regarding with the customer's viewpoint. The possibility of arbitration in case of legal disputes can be also considered.

"Indemnifications" can be described when services are not properly provisioned according to their TS. They are just as the aforementioned compensations, so that if TS or privacy policies are violated, customers may be entitled to terminate the contract relationship.

2.4 Privacy Policy

The "Privacy Policy" (PP) refers to regulations on customers data management as Figure 4 denotes. A most important and controversial point regarding PPs is the jurisdiction to be applied in case of data breaching. This is due to different locations may have different data protection regulations. Thus, for instance, EU and US have very different approaches, being the European countries much more protective. Currently, the US-EU Privacy Shield Framework from 2016 establishes legal mechanisms to transfer personal data. PPs consider data-related topics such as integrity, preservation, disclosure, location, ecological quality datacenters, and monitoring.

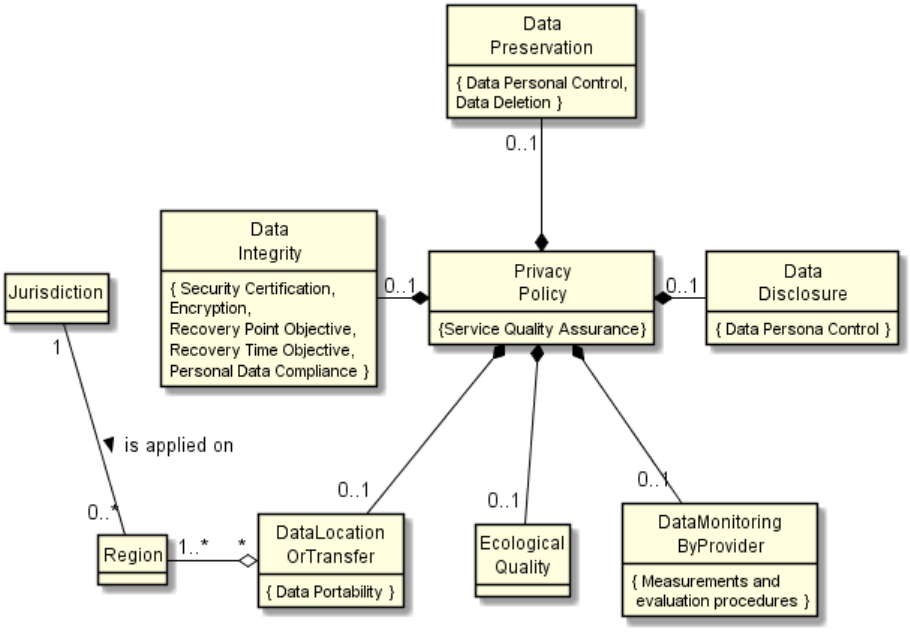

Fig. 4. Model for privacy policy.

"Data integrity" considers security certification and encryption (possibly applying standards and external auditory, on data storage, transport, and key management), recovery point or time management, and personal data compliance (certified data protection standards and auditory).

"Data preservation" comprises personal data control and data deletion. According to EU jurisdiction, there are concerns if providers control or uses personal data. Providers may offer their customers a grace period for accessing to their data once contracts are terminated. Regarding with data deletion, providers may offer deletion with or without post-recovery techniques to ensure that data is properly erased.

"Data disclosure" refers to the providers attitude to share personal data with third parties. As an example, this is usually the case of chat services. If a customer writes a message, this data must be transferred to the messenger in order to be dispatched. However, most usually, personal data can not be disclosure except at law court requests, with or without notice to customers. These options depends deeply upon jurisdictions.

"Data location or transfer" includes data portability encryption, and backup location. Data retrieving may be either not possible, or be physically carried out, or be transferred through an API in a suitable (or not) format for customers. Regarding data location and their backups, EU regulations impose data from public organizations to be located on datacenters physically located on EU or, if not, ruled on EU directives.

"Ecological quality datacenters" refers to datacenters powered by neutral carbon or renewable power supply. Optionally, providers may publish information about their CO2 emissions and offer ways for customers to check.

"Data monitoring" by providers includes measurement and evaluation procedures. Usage data may be aggregated to search patterns for services to be improved, or enforcing the user acceptable policies, with or without notice to customers.

3 Operational Agreements

In general, agreements play a crucial role in society where they act as the trustworthy connectors amongst peers in business transactions regulating the rights and responsibilities of the stakeholders. In such a context, the model presented represents a foundation for explicit operational agreements that can be leveraged as first class citizens that contains the knowledge to regulate an automated governance of IT infrastructures and embrace dynamic liaisons amongst organizations in the context of Cloud Services.

From this perspective, the Customer Agreement could be seen as an operational asset that can be managed and exploited to support a wide range of decisions in an automated fashion: from low level technical capacity management policies in the infrastructure, to the business model regulated in the executive layer. This operationalization could potentially involve both fully-autonomous and semi-automated components. As an example, on the one hand we can have automated testing platforms that analyze the expected SLAs of the cloud provider to automatically detect whether the system behaves in a fulfilling way; on the other hand, in order to design the pricing model for the SaaS customers, a supporting tool to analyze the different alternatives can assist the executive layer, so the decisions over that pricing model are done in a systematic and informed way.

As a promising consequence of this evolved notion of operational Customer Agreements, we would be in the verge to integrate business models as an operational asset that would allow a leverage of information systems from a pure technical level to a business-driven ecosystem of cloud services.

4 Related Work

The legal surveys on cloud computing which have been our sources for the reference model are: (1) a comparison and analysis of contracts for clouds [8] written by members of the School of Law at Queen Mary London University, and the Internet Institute at University of Oxford. It includes a study of compliance of some cases to EU and US regulations; (2) the final report for the European Commission about standards terms and performance criteria in SLAs for cloud computing services [11], which presents a SLA model to provide some further stability, certainty and transparency in the cloud market; and (3) the NIST roadmap to adopt cloud technologies in the US Government and also corporations in the US [4].

Besides of the previous works, [2] presents a systematic analysis on privacy policies from different regulations, written by members of the University of Cardiff. They proposed a Combined Privacy Law Framework (CPLF) including key principles for privacy policies and individual rights, which constitutes the basis for a *Privacy by Design* approach, but leave both terms of service and service-level agreement out-of-scope.

Regarding with automating the compliance in cloud computing and also other areas, there are some recent papers which introduce how to automate the GDPR compliance in cloud-hosted services [6, 7] and online healthcare [5] by applying timed transition systems, blockchain, and smart contracts, respectively. In [3] a review of several approaches for automated compliance checking is presented in the area of building environments. In [13] a similar approach in healthcare building design is presented.

5 Conclusions

In this paper, we have introduced a reference model which will be the cornerstone of further research for achieving a higher operationalization degree of customer agreements, including the compliance checking with respect to legal jurisdictions, in order to complement the existing analysis operations that mostly focus on SLAs and pricing terms. This model enables the terminological alignment of customer agreements, so that both providers and customers can specify and analyze legal aspects of cloud services. We plan to further extend this preliminary work by validating the model with actual service offerings, and by devising additional analysis operations applied to terms of service and other legal aspects of customer agreements.

References

1. Al-Roomi, M., Al-Ebrahim, S., Buqrais, S., Ahmad, I.: Cloud Computing Pricing Models: A Survey. International Journal of Grid and Distributed Computing **6**(5), 93–106 (2013). https://doi.org/10.14257/ijgdc.2013.6.5.09, `http://dx.doi.org/10.14257/ijgdc.2013.6.5.09`

2. Aljeraisy, A., Barati, M., Rana, O., Perera, C.: Privacy Laws and Privacy by Design Schemes for the Internet of Things. ACM Computing Surveys **54**(5), 1–38 (6 2022). https://doi.org/10.1145/3450965
3. Amor, R., Dimyadi, J.: The promise of automated compliance checking. Developments in the Built Environment **5**, 100039 (3 2021). https://doi.org/10.1016/j.dibe.2020.100039
4. Badger, L., Bernstein, D., Bohn, R., de Vaulx, F., Hogan, M., Iorga, M., Mao, J., Messina, J., Mills, K., Simmon, E., Sokol, A., Tong, J., Whiteside, F., Leaf, D.: US Government Cloud Computing Technology Roadmap. Tech. rep., National Institute of Standards and Technology, Gaithersburg, MD (10 2014). https://doi.org/10.6028/NIST.SP.500-293, `https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.500-293.pdf`
5. Barati, M., Aujla, G.S., Llanos, J.T., Duodu, K.A., Rana, O.F., Carr, M., Ranjan, R.: Privacy-Aware Cloud Auditing for GDPR Compliance Verification in Online Healthcare. IEEE Transactions on Industrial Informatics **18**(7), 4808–4819 (7 2022). https://doi.org/10.1109/TII.2021.3100152
6. Barati, M., Rana, O.: Checking GDPR Compliance for Cloud-based Services. In: 2021 IEEE World Congress on Services (SERVICES). pp. 2–2. IEEE (9 2021). https://doi.org/10.1109/SERVICES51467.2021.00013
7. Barati, M., Theodorakopoulos, G., Rana, O.: Automating GDPR Compliance Verification for Cloud-hosted Services. In: 2020 International Symposium on Networks, Computers and Communications (ISNCC). pp. 1–6. IEEE (10 2020). https://doi.org/10.1109/ISNCC49221.2020.9297309
8. Bradshaw, S., Millard, C., Walden, I.: Contracts for clouds: comparison and analysis of the Terms and Conditions of cloud computing services. International Journal of Law and Information Technology **19**(3), 187–223 (9 2011). https://doi.org/10.1093/ijlit/ear005
9. Garcia, J.M., Martin-Diaz, O., Fernandez, P., Muller, C., Ruiz-Cortes, A.: A Flexible Billing Life Cycle for Cloud Services Using Augmented Customer Agreements. IEEE Access **9**, 44374–44389 (2021). https://doi.org/10.1109/ACCESS.2021.3066443
10. García, J.M., Martín-Díaz, O., Fernandez, P., Ruiz-Cortés, A., Toro, M.: Automated analysis of cloud offerings for optimal service provisioning. In: Service-Oriented Computing: 15th International Conference, ICSOC 2017. vol. 10601 LNCS, pp. 331–339. Springer (11 2017). https://doi.org/10.1007/978-3-319-69035-3_23, `http://link.springer.com/10.1007/978-3-319-69035-3_23`
11. Hans Graux, Jos Dumortier, Patricia Ypma, Jasmine Simpson, Peter McNally, Marc de Vries: Digital Agenda for Europe Standards terms and performance criteria in service level agreements for cloud computing services. Tech. rep., European Union, 2015 (2013). https://doi.org/10.2759/07446
12. Müller, C., Fernandez, P., Gutierrez, A.M., Martín-Díaz, O., Resinas, M., Ruiz-Cortés, A.: Automated Validation of Compensable SLAs. IEEE Transactions on Services Computing (2018). https://doi.org/10.1109/tsc.2018.2885766
13. Soliman-Junior, J., Tzortzopoulos, P., Baldauf, J.P., Pedo, B., Kagioglou, M., Formoso, C.T., Humphreys, J.: Automated compliance checking in healthcare building design. Automation in Construction **129**, 103822 (9 2021). https://doi.org/10.1016/j.autcon.2021.103822
14. de Vaulx, F., Simmon, E., Bohn, R.: Cloud computing service metrics description. Tech. rep., National Institute of Standards and Technology, Gaithersburg, MD (4 2017). https://doi.org/10.6028/NIST.SP.500-307, `http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.500-307.pdf`