State of the art and challenges of security SLA for cloud computing

Carlos André Batista De Carvalho, Rossana Maria de Castro Andrade, Miguel Franklin de Castro, Emanuel Ferreira Coutinho, Nazim Agoulmine

State of the art and challenges of security SLA for cloud computing

Carlos André Batista de Carvalho [a,b,c,*], Rossana Maria de Castro Andrade [a,b], Miguel Franklin de Castro [a,b], Emanuel Ferreira Coutinho [b], Nazim Agoulmine [d]

[a] *Graduate Program in Computer Science (MDCC), Federal University of Ceará (UFC), 60440-900, Brazil*
[b] *Group of Computer Networks, Software Engineering, and Systems (GREat), 60440-554, Brazil*
[c] *Computer Science Departament, Federal University of Piauí (UFPI), 64055-490, Brazil*
[d] *IBISC Laboratory, University of Evry, 91034, France*

There are users and organizations that resist adopting cloud computing solutions, due to concerns about the security and privacy of their data. A Service Level Agreement (SLA) can be used to address these concerns, increasing trust in the purchased services through the clear description of the guarantees offered by the provider to the subscribers. For this purpose, the authors performed a literature systematic mapping to enumerate existing solutions and open issues in security SLAs in cloud computing. This review is presented in this paper as well as an analysis of the state of art. This paper also presents a classification of the selected papers and a discussion about management of security SLAs in clouds.

1. Introduction

Cloud computing is a paradigm that allows companies and organizations to focus their efforts on their core business or activity by outsourcing its resources in Information Technology (IT). Cloud computing makes it possible to reduce the infrastructure cost by contracting a public cloud provider and paying only for the consumed resources. Elasticity is one of its main features as it allows the use of more or fewer resources in accordance with the needs. Cloud computing is a reality, with high investments from big companies, such as Amazon, Microsoft, and Google. However, this technology comes with the main drawback that is the loss of control over the cloud infrastructure. Consequently, individuals, companies, and organizations are resisting adopting public clouds, due to concerns about the security and privacy [1,2].

Rong et al. [3] highlight security challenges related to, for example, data leakage, data sharing, resource location, availability and multi-tenancy issues. The providers deal with the security concerns, implementing controls based on standards and frameworks, such as ISO/IEC 27017[1], Cloud Security Alliance's Cloud Control Matrix (CSA CCM)[2] and US National In-

☆ Reviews processed and recommended for publication to the Editor-in-Chief by Area Editor Dr. G. Martinez.

* Corresponding author at: Computer Science Departament (SG-9), Federal University of Piauí (UFPI), Campus Universitário Ministro Petrônio Portella, Ininga, Teresina/PI 64049-550, Brazil.

E-mail addresses: candrebc@ufpi.edu.br (C.A.B.d. Carvalho), rossana@ufc.br (R.M.d.C. Andrade), miguel@great.ufc.br (M.F.d. Castro), emanuel@virtual.ufc.br (E.F. Coutinho), Nazim.Agoulmine@ufrst.univ-evry.fr (N. Agoulmine).

[1] http://www.iso.org/iso/catalogue_detail?csnumber=43757.

[2] https://cloudsecurityalliance.org/group/cloud-controls-matrix/.

stitute of Standards and Technology (NIST) Special Publication 800-53[3] [2]. These frameworks can be used to assess the providers, increasing the trust in their services. However, the customers have only a view of the cloud security and require mechanisms that supply security assurances and greater transparency over the provided services [2].

In this context, Service Level Agreements (SLAs) can be used to provide the desired transparency and guarantees. An SLA is a formal document in which a cloud provider specifies its level of QoS assurance through the parameters of the non-functional requirements (e.g., availability, performance and security) [4]. For example, it is possible to define that a service will be available 99.9% of the time and a response time be, at most, 3.5 s. However, security terms are not covered in SLAs of the public cloud providers [3]. For example, the Amazon EC2 SLA only specifies service availability[4], without any other QoS assurance. Likewise, Microsoft[5] and Google[6] provide only availability assurances.

A solution of security SLA for clouds must include tools to manage an SLA, allowing the negotiation of the SLA terms in accordance with the customer's needs, and assessment and measurement of the security in a cloud environment. Audit mechanisms are important to avoid that tampered information are provided. When a violation of some SLA term is detected, procedures can be performed to restore an SLA.

Faniyi and Bahsoon performed a systematic review about the SLAs management in the cloud environment [5]. Their focus is the analysis of the resource allocation techniques that can be used to maintain the SLA. However, they do not address security aspects in their analysis. Luna et al. [2] discuss the standardization of the security SLA, and Casola et al. [1] analysis the research initiatives and open issues, considering mainly their previous contributions. Besides, review papers, about cloud security, do not properly address the SLA management [3].

In this context, we performed a systematic mapping of the literature to search for solutions of security SLAs for clouds and for existing challenges. The main contribution of this paper consists of analyzing the state of the art in security SLA management for clouds. The aims of this review are: i) identify and classify the contributions of security SLA for clouds; and ii) discover limitations of existing solutions and research opportunities. The results of our review are presented here with a discussion about the management of the security SLA and open issues.

The remaining of this paper is organized as follows. In Section 2, we present the SLA components and the life cycle of an SLA, focusing in the cloud security context. The systematic mapping is exposed in Section 3. We summarize the open challenges in Section 4 and the conclusions at the end of this paper.

2. Security SLA for cloud computing

An SLA is a legal contract that defines the QoS offered by a provider as part of agreements with the customer contracting [5]. The main components of an SLA contract are the Service Level Objectives (SLOs) that are inherent to the aspects covered by the SLA. Each SLO contains a set of Service Level Indicators (SLIs), which should be measured to determine the QoS level [6]. Other elements should be described to indicate the limitations of the provided services, eliminating unrealistic expectations, and the penalties to indemnify the customers in case of violations. Due to changes in the environment, it is possible to define when and how an SLA can be re-negotiated [1]. In the Cloud Computing context, an SLA may, in addition, specify the billing model [7], the contingency plan for disaster recovery [8] and legal aspects related, for example, to the data location [9].

An SLA has a life cycle to perform the SLA management. This life cycle starts with the identification of terms and finishes with the end of the relationship between the parties. There are different terminologies to define the SLA life cycle's phases. In this paper, we use the definition presented by Bose et al. [4], which consists of the following five phases:

1. *Contract definition*: A provider defines a set of services and their SLAs, using templates;
2. *Publishing and discovery*: A provider announces the services and the clients search the offers that satisfy their needs;
3. *Negotiation*: When a suitable provider is found, the parties have to agree with the SLA terms. Thus, they use a negotiation protocol in which the client lays out the desired QoS and the provider analyzes if it can comply with this request. Currently, there are efforts to automate the SLA negotiation in clouds [10,11];
4. *Operationalization*: After the SLA signature, the operationalization starts with the SLA monitoring, accounting and enforcement. In the monitoring, the SLIs are measured and compared with the agreed values, allowing the detection of SLA violations. In the case of a violation, it can be reported and a penalty can be applied. Casola et al. [1] include, in this phase, the remediation and re-negotiation activities to restore an SLA; and
5. *De-commissioning*: At the end of the relationship between the parties, the termination is performed according to the terms and conditions defined in the SLA.

It is important to highlight that an SLA can be used in other contexts, such as grid computing and web services. The SLAs of the public cloud providers usually specify only the service availability, and other SLA proposals do not cover security aspects. Bose et al. [4], for example, enumerate metrics such as response time, throughput, latency, and availability.

[3] http://csrc.nist.gov/publications/drafts/800-53-rev4/sp800-53-rev4-ipd.pdf.
[4] http://aws.amazon.com/ec2/sla/
[5] http://azure.microsoft.com/en-us/support/legal/sla/.
[6] https://cloud.google.com/appengine/sla.

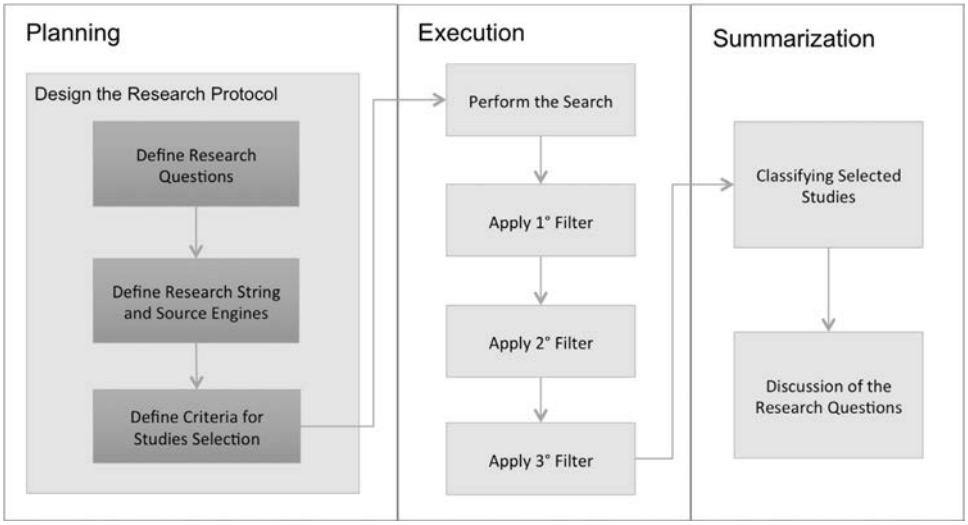

Fig. 1. Systematic mapping process.

On the other hand, Chaves et al. [8] proposed some security metrics to be used in SLA contracts, however, these metrics are generic and they do not consider cloud computing features. The backup policies, repair time and password management are examples of metrics proposed by them.

It is important to highlight that both clients and providers are responsible for cloud security and the security requirements can vary in accordance with the used service and deployment models. These aspects must be considered in an SLA definition. Besides, a security SLA for clouds must consider the clients' needs and the existing threats in this environment. The Cloud Security Alliance (CSA)[7] published a document with the most significant threats in clouds [12].

The SLA negotiation protocol is important to comply with different security requirements. For example, a client can pay more for a service that provides a Trust Platform Module (TPM) to increase its data security. Another example is the provisioning of services in the location with the lower cost if the client does not have the restriction for the data and applications location.

After the negotiation, the monitoring is performed to measure the QoS. Thus, it is possible to verify if the signed SLA is being fulfilled and execute procedures to repair the SLA in cases of violations. The auditing is an important activity to prove the occurrence or not of SLA violations. Lastly, an SLA solution should comply with the cloud requirements (e.g., elasticity) and should not degrade the system performance.

We found some studies that aim at defining security SLAs for cloud computing. We perform a review of the literature to conceive a holistic vision of security SLA for clouds. Therefore, research questions are identified and solutions are presented.

3. Systematic mapping

We used the systematic mapping mechanism to perform the literature review. It is a mechanism of bibliographic review that produces, as a result, the general vision of a research topic. In this review type, it is possible to classify the selected studies and to identify evidences for future work. The review is conducted by a protocol that can be replicated and updated.

We executed the systematic mapping in accordance with a process detailed in Fig. 1. This process contains three steps: **Planning, Execution**, and **Summarization**. In the Planning step, the research protocol is created. This protocol contains the research questions, search strings, source engines, and selection and exclusion criteria. The criteria are applied on the filters to select only relevant results. These filters, which are described in next subsection, are executed after obtaining the primary studies from the search engines. Lastly, the data extraction is performed with the selected studies, summarizing the results of the review. In the rest of this section, the protocol used, the studies classification, and the discussion of the research questions are detailed.

3.1. Systematic mapping protocol

The definition of the research questions is an important task in the creation of the review protocol since they are used to guide the review and aid to achieve their aims. After a preliminary analysis of the literature, we prepared the following research questions:

[7] https://cloudsecurityalliance.org.

Table 1
Search strings used in the systematic mapping.

Search engine	Search string
IEEE Xplorer	"Document Title":secure OR "Document Title":security OR "Document Title":privacy OR "Abstract":secure OR "Abstract":security OR "Abstract":privacy) AND ("Document Title":cloud OR "Abstract":cloud) AND ("Document Title": sla OR "Document Title":slas OR "Document Title":"level agreement" OR "Document Title":"level agreements" OR "Abstract":sla OR "Abstract":slas OR "Abstract":"level agreement" OR "Abstract":"level agreements")
Science Direct	(TITLE-ABSTR-KEY(security) or TITLE-ABSTR-KEY(secure) or TITLE-ABSTR-KEY(privacy)) and TITLE-ABSTR-KEY (cloud) and (TITLE-ABSTR-KEY(sla) or TITLE-ABSTR-KEY (slas) or TITLE-ABSTR-KEY("level agreement") or TITLE-ABSTR-KEY("level agreements"))
Scopus	(TITLE-ABS-KEY(security) or TITLE-ABS-KEY(secure) or TITLE-ABS-KEY(privacy)) and TITLE-ABS-KEY(cloud) and (TITLE-ABS-KEY(sla) or TITLE-ABS-KEY(slas) or TITLE-ABS-KEY("level agreement") or TITLE-ABS-KEY("level agreements"))
Google Scholar	tudonotítulo: (cloud (security OR secure OR privacy) (sla OR slas OR "level agreement" OR "level agreements"))

- **RQ1:** *How is security treated in SLAs for cloud computing?* In this question, we must analyze how the SLA's parameters are defined and measured. Besides, it is important to detect the threats addressed in found solutions.
- **RQ2:** *How is the negotiation of the security parameters performed?* This question identifies the elements used in SLA negotiation as well as the languages for SLA representation. The SLA's language is a key aspect of enabling an automated negotiation.
- **RQ3:** *What are the features observed in SLA operationalization?* During the operationalization phase, some activities are performed, especially the monitoring and auditing. Here, we observe who is responsible for these tasks and what data are collected. Besides, it is important to verify the link with the negotiation process and the other activities involved in order to not only detect some violation but restore the SLA.
- **RQ4:** *How are the solutions deployed and evaluated?* It is interesting to observe the evaluation methods used to validate each solution and the deployment in real clouds, identifying the service and deployment models, and the tools used in found solutions. Here it is also possible to detect the existing limitations.

The search string was built with the combination of the keywords **Security, Cloud** and **SLA** and their synonyms. The keys terms are queried in title, abstract and keywords of the publications. The research was performed in the IEEE Xplorer[8], Science Direct[9], Scopus[10] and Google Scholar.[11] In Google Scholar, the search was restricted to the title, because of the limitations of the automatic search tool. Each search engine has its own search language and Table 1 shows the strings used in each tool.

In the Execution step, three filters were applied to select only works that answer the research questions. In the first filter, we excluded any duplicated studies (i.e., studies found in many engines) and the unavailable works. The search eventually returned results without content (e.g., keynotes and proceedings abstracts), which also were removed in this filter. For applying the second filter, we read the abstract of the papers that passed the previous filter. Then, we selected only works that had initiatives related to the use of SLA for security in the context of cloud computing. In the third filter, we selected the studies that provide answers to our research questions. To apply the last filter, it was necessary to read the full paper. The analysis in second and third filters is subjective, and the papers were selected when in doubt. While reading each paper, we look for mainly the activities of the SLA management and the security issues addressed. After the protocol execution, in the Summarization, we analyzed the selected studies to perform the classification of the works and to discuss the research questions.

3.2. Results and classification of studies

In this subsection, we show the results of the review and present a classification of selected works. This review finished at end of 2015 and followed the previous protocol. We found 494 works: 111 in IEEE Xplorer; 17 in Science Direct; 311 in Scopus; and 55 in Google Scholar. With the first filter, we removed 238 works: 135 studies duplicated; 55 results without content; and 48 unavailable works. Thus, we selected 256 works for the second filter.

We observed that some studies are out of this research scope, after reading the abstract. These works do not focus on security SLAs for clouds. In the second filter, we excluded 87 works and selected 169 works for the third filter. In the last filter, 87 studies were removed because they do not answer to any research question. Thus, 82 papers were selected for the summarization step.[12]

Fig. 2 shows the number of selected studies published by year, considering also the publishing type. We can see the increased interest of the academic community into the subject starting from 2011. The research studies were published

[8] http://ieeexplore.ieee.org/Xplore/home.jsp.
[9] http://www.sciencedirect.com.
[10] http://www.scopus.com.
[11] https://scholar.google.com.
[12] Due to space limitations, the list of selected works in each step can be accessed at: https://sites.google.com/site/candrebc/systematic-mapping-secla.pdf.

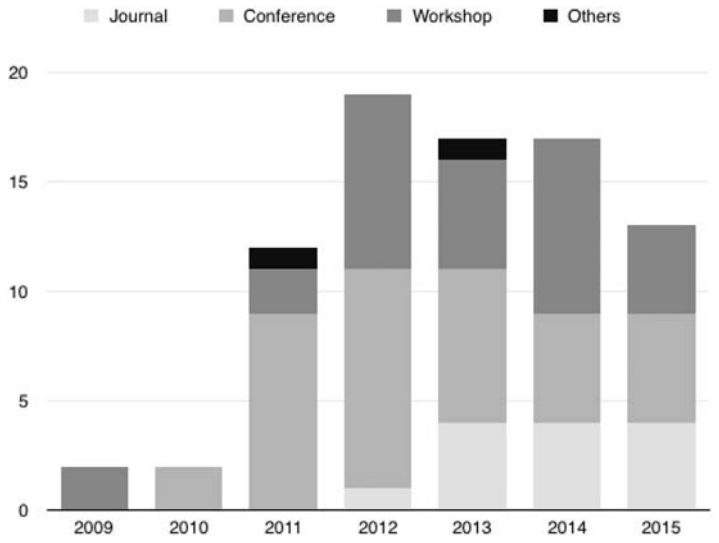

Fig. 2. Number of papers by year and publishing type.

Table 2
Number of publications by conferences and journals.

Conference or journal	Quantity
International Conference on Cloud Computing Technology and Science (CloudCom)	7
International Conference on Cloud Computing and Services Science (CLOSER)	7
IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)	3
ACM Cloud Computing Security Workshop (CCSW)	2
IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGrid)	2
IEEE International Conference on Cloud Computing (IEEE CLOUD)	2
IEEE International Conference on Cloud Computing in Emerging Markets (CCEM)	2
International Conference on Availability, Reliability and Security	2
International Conference on Computational Aspects of Social Networks (CASoN)	2
International Journal of Security and its Applications	2
International Workshop on Security and Privacy Engineering (SERVICES SPE)	2

mainly as conference papers, which represent 82% of the selected studies (i.e., 67 papers). Of this total, 38 research studies were published in technical sessions and 29 works were published in satellite events such as posters and workshops.

The increase of publications in journals, since 2013, indicates the maturity and importance of this topic. Despite the slight reduction in the number of paper published in 2015, we believe that there are works in progress to be published and that the topic is still relevant. We can highlight, for example, the recent studies that underline efforts for standardization [2] and the open challenges [1]. Besides, the last time we made the queries in search engines was in December 2015, and their databases were probably later upgraded.

There were 58 different conferences and journals. We can highlight the IEEE International Conference on Cloud Computing Technology and Science (CloudCom) and the International Conference on Cloud Computing and Services Science (CLOSER). In each conference were selected seven publications. Next, we underline the IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), with three publications. Table 2 shows the conferences and journals with, at least, two publications.

Researchers of 26 countries published their studies about the use of SLA for cloud security. Fig. 3 displays the number of paper by country. Researchers from different countries participated in some publications. Thus, some papers have been accounted for more than one country. Countries with the largest numbers of publications are Germany, USA and Italy, with 13, 11 and 10 publications respectively.

In a detailed analysis, we observe the participation of 70 research groups in the selected papers, and that few groups obtained several publications. In some papers, more than one group collaborated in the research study. We can highlight the research projects SPECS (Secure Provisioning of Cloud Services based on SLA management) and mOSAIC (Open-Source API and Platform for Multiple Clouds) since we selected fifteen works with researchers involved in these projects. These are researchers from one of the following universities: Second University of Naples, University of Naples Federico II, University of Sannio, Technical University Darmstadt, West University of Timisoara and University of Catania. OPTIMIS (Optimized Infrastructure Services) and CLOVIS (Cloud Computing Improvement through Risk and SLA Management) are others projects that address the use of SLA for cloud security.

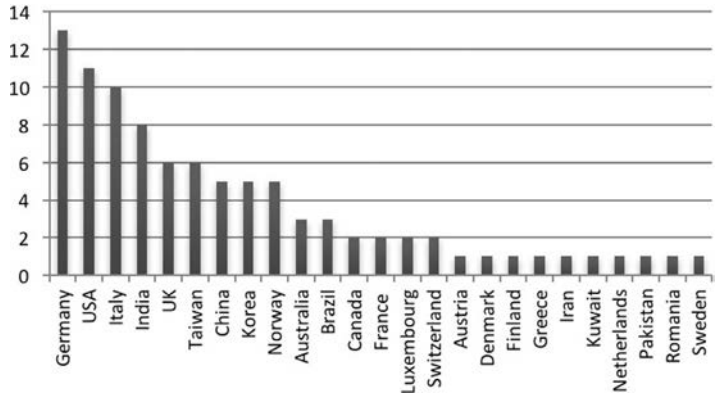

Fig. 3. Number of papers by country.

We observed that the selected studies do not consider all parts of the SLA life cycle. Thus, we classified the papers in accordance with the life cycle phase they address. Normally the **negotiation** or **operationalization** are addressed in these works, but 21 works consider both phases. Some studies show important elements of an SLA (e.g., security parameters or language for SLA representation), without analyzing others phases of the SLA life cycle. We only classified these studies in the **definition** phase.

The **publishing and discovery** phase was not considered in the classification, although there are some studies that address this phase [6]. This phase was not considered because we focused on negotiation and operationalization. Besides, we believe this phase of the SLA life cycle is not an open challenge in cloud security.

On the other hand, the SLA **de-commissioning** is an important phase that is not addressed in selected studies. A single paper was found, showing a system to ensure the client data destruction at the end of the contract [13]. However, it is necessary to offer other guarantees, allowing the service migration to another provider or user data and applications backup when the contract is ended.

Furthermore, we did an analysis of solution deployment in real clouds. We can classify these studies in accordance with the **solution type. Experimentation** is the category of 18 works, representing 21.95% of the studies. Only one research study used a cloud **simulator** [14], which can characterize the difficulty of representing the solutions in simulators.

Some works contain proposals of, for example, a mechanism for SLA evaluation, a negotiation protocol or a monitoring system. Since these solutions have not been deployed in real clouds, the term **solution proposal** was used to classify these studies. The remainder of the works was classified into **conceptual model** for introducing, for example, an architecture [2], a framework [6] or a model [15], without specifying any concrete proposal.

In this context, we did a mapping of the selected works in accordance with the phases of the SLA life cycle and the solution type, resulting in an overview of research studies about security SLA for clouds. Fig. 4 displays the mapping with the number of papers by category.

By analyzing the mapping, we observe that an important number of studies focuses only on the operationalization. There are works that analyze superficially a specific phase of the SLA life cycle, but detail a solution for another phase. In these cases, the classification considers only the phase treated in depth. For example, Bernsmed et al. [6] define a negotiation process but only indicate the monitoring goals. Thus, only the negotiation phase was considered when classifying this research study.

The mapping displays fourteen papers (i.e., 17.07%) that address only SLA definition for cloud security. These papers specify, for example: security metrics; questions to be answered in an SLA; language for SLA representation; and security SLA requirements. These works do not detail a proposal to enable the use of security SLA and were classified as conceptual model.

It is interesting to point out that experimentation is mainly conducted in works about SLA operationalization. The negotiation proposals have not been deployed in real clouds. Most of these studies propose a solution to evaluate SLA of different providers. The difficulty to implement a system, interacting with real clouds, makes impracticable the experiments.

The studies that address both the negotiation and operationalization are mostly superficial, without details to enable the deployment in real clouds [1,8]. We found only six papers that show experiments and detected some limitations in the analysis of these papers. For example, Ficco et al. [16] treat a specific scenario of intrusion detection. In Binu and Gangadhar [17], the cryptography is used to protect the logs, but the monitored parameters do not express the security of the environment. Only the number of daily logins and unsuccessful logins are monitored in the solution proposed by Almorsy et al. [18]. In others papers, essential details are omitted (e.g., the metrics used and the formulas applied in monitoring).

On the other hand, some research studies address a single phase of the SLA life cycle in a specific context. In these cases, we found suitable solutions, treating, for example, the data location [9], data breaches [19], or providers' assessment [20].

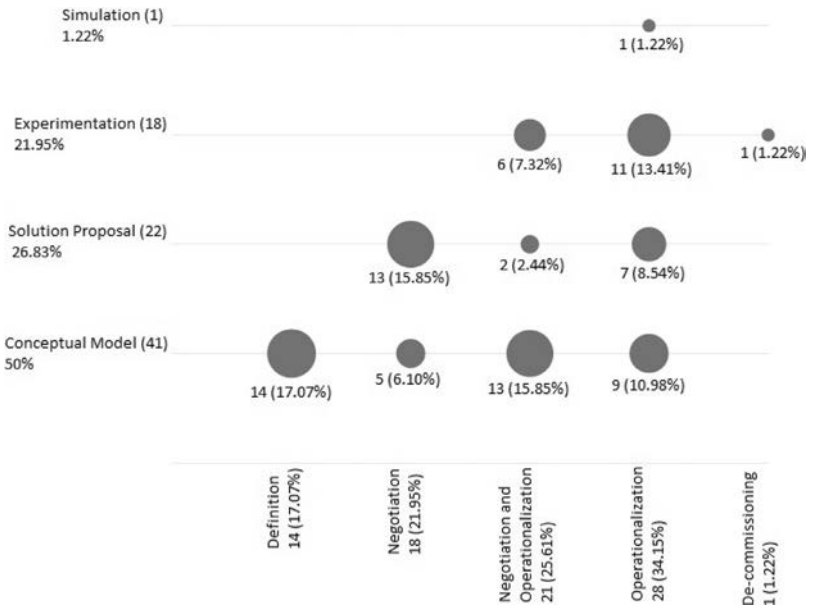

Fig. 4. Classification of studies in accordance with the SLA life cycle phase and the solution type.

3.3. Discussion of the research questions

The discussion of the research questions, shown in this Subsection, completes the previous classification with a comprehensive vision of the state of the art.

3.3.1. How is security treated in SLAs for cloud computing?

Firstly, it is necessary to detect the user's concerns about cloud services. In this review, we found some threats related to this environment. The cited threats, in accordance with the CSA classification [12], are: shared technology vulnerabilities; insufficient due diligence; data breaches or data loss; and Denial of Service (DoS).

In this context, there are works that use the SLA to mitigate some specific threat. Raj et al. [21], for example, propose a solution to ensure data isolation in a shared infrastructure and Ficco et al. [16] designed a service for intrusion detection. Studies about secure storage are concerned with data breaches [19,22]. While Popa et al. [19] focus on the data integrity, Chuang et al. [22] treat the data leakage. Another concern is related to legislative requirements for the data location in the cloud. Albeshri et al. [9] propose an approach to ensure the location where the data is stored while proving its possession.

Some selected works highlight the threat of insufficient due diligence [7,15]. This threat is related to the transfer of responsibility from the cloud control and cloud security to the provider. Thus, the clients can take unknown risks, due to the lack of transparency inherent to the security mechanisms applied by a provider. This lack of transparency brings, for example, questions about the billing services [7]. Generally, the studies about SLA operationalization aim to increase the transparency of the services offered.

The security SLA parameters should be defined based on the existing threats. In the selected works, we found parameters extracted from security policies [8], laws [23] or cloud security guidelines [20,24]. Generally, the SLA is represented in a known language, such as Web Service-Agreement (WS-Agreement). In this context, it is essential to define a vocabulary that expresses the SLA terms and their relationship with the security controls.

It is important to assign values to the SLA parameters. These values can be calculated during the operationalization [18,25] or can be used to evaluate the security of a provider during the negotiation [20]. Chaves et al. [8] highlight the difficulty of measuring security. Some researchers choose to use binary values, which may, for example, reflect the use of a specific security mechanism [6]. Other works use discrete values representing different security levels [25].

3.3.2. How is the negotiation of the security parameters performed?

Most of the works about SLA negotiation focus on processes for selection of services or providers. Zhengwei et al. [20], for example, propose a method to select a provider in accordance with the client needs. In this case, the security is analyzed based on reports from the CSA STAR (CSA Security, Trust and Assurance Registry) program.[13] There are research studies about services selection applied in hybrid or federated clouds [6]. In another approach, the client negotiates the desired

[13] https://cloudsecurityalliance.org/star/.

security with a provider [17]. In this type of work, the provider can present an SLA template to be used by clients as support for negotiation.

The use of a machine-readable language allows the automation of the negotiation process, and Meland et al. [11] show the possibility of expressing the security requirements in ten languages. However, the language WS-Agreement is the most used in the found research studies. Guesmi and Clemente [10] exhibit the detection of conflicting requirements with a machine-readable language. A language can also be used to facilitate the communication between the clients and providers, due to differences in expressing, respectively, security needs and offers.

Besides a language, it is necessary to define a protocol to describe the negotiation process. One protocol example is defined by Bernsmed et al. [6]. In this protocol: i) the client sends a message to the broker, describing the security requirements of each cloud service; ii) the broker verifies which providers offer each service, and requests their SLAs; iii) after receiving the providers' answers, the broker runs a decision mechanism to select which provider will execute each service; and iv) the broker informs, to the client, the result of the negotiation process. In relation to the decision mechanism, we found works that make a cost analysis [14], and verify the clients' priorities, described by weighting [20].

3.3.3. What are the features observed in SLA operationalization?

In relation to SLA operationalization, we identified proposals for auditing that allow increasing the trust in cloud providers. It is possible to introduce a Third-Party Auditor (TPA) or Trusted Third-Party (TTP) in order to aid the auditing process [15]. Another possibility is the use of secure logs [19], providing, with digital signatures, the integrity and non-repudiation of the cloud transactions [7,19]. The auditing proposed in the selected research studies does not necessarily monitor security parameters. It is possible, for example, to audit the consumed resources to provide a trust billing system [7].

During the operationalization, it is necessary to verify if the monitored parameters are in accordance with the contracted SLA. The parameters monitoring can be done by the provider [1,25], using monitoring agents. However, a customer can claim that a provider has tampered with the information about the quality of the provided service [15]. Thus, Park et al. [7] suggest the use of a TPM to supply greater security of the monitoring solution. Another approach is the utilization of a TPA, despite its limitations [15]. For example, a third party cannot capture the information extracted from a virtual machine about the used resources. In a monitoring solution, it is even necessary to define a monitoring interval that does not diminish the system performance [1].

We can highlight the monitoring solutions that focus on specific contexts, such as resource isolation [21] and intrusion detection [26]. Moreover, there are scenarios where the monitored parameters are different from the negotiated parameters. For example, in the security storage context, a client can request that his data must be stored at a specific location. In this case, the response time could be monitored to infer the distance between the parties, and therefore the data's location [9]. The relationship between these parameters must be proved, and so an audit is performed to demonstrate compliance with the negotiated requirements.

Besides the service monitoring, it is possible to perform procedures for SLA reestablishment if an SLA violation was detected. This behavior was found in some studies in the context of federated clouds [6,27]. In this type of work, there is a possibility of migrating the services [6] or the virtual machines [27] for the conservation of the SLA. There is a concern with the SLA re-establishment in others research studies. Doelitzscher et al. [26], for example, propose to put in quarantine the virtual machine and to start a new virtual machine when an intrusion is detected. However, the violation management normally is not treated [18]. Besides, in monitoring tools analyzed by Petcu and Craciun [28], only an alert is generated when an SLA violation is detected. The SLA re-negotiation is performed to modify the SLA previously signed, allowing the client to change his requirements, and also the SLA reestablishment [1].

Lastly, we need to show that the SLA parameters were not always detailed in the research studies selected. In the research performed by Casalicchio and Silvestri [27], it is stated that a meta-metric admit values between 0 and 1. However, besides the shown examples, it is not detailed how to measure these values. Djemame et al. [23] proposed another approach with metrics calculated based on a specialist opinion. This approach is disadvantageous because it adds a subjective factor, making unfeasible any automatic measurement. Nevertheless, we highlight the researches done by Chauhan et al. [24] and by Silva and Geus [25] that perform security measurements in their experiments. For example, Chauhan et al. define, as metrics, the percentage of the system affected by incidents and the percentage of time that services were unavailable, and determine how the latter is calculated [24].

3.3.4. How were the solutions deployed and evaluated?

Besides the analysis of the SLA negotiation and operationalization, we observed how the proposed solutions were evaluated. We identify four categories: informal discussion, formal proof, description of real or hypothetical scenarios, and performance analysis. However, almost half of the studies (45.12%) do not make references to an evaluation method. Table 3 shows this classification. Some works use more than one evaluation type [19,26]. Popa et al. [19], for example, exhibit a formal proof and a performance evaluation of their proposal.

Many studies about SLA negotiation use the description of hypothetical scenarios for the evaluation. Usually, these scenarios simulate a client needs and the provider offers, allowing the selection of the most suitable provider [6]. Real scenarios were mostly used in works about SLA operationalization and with experiments [25]. The discussion of the solutions was performed to present the security or the scalability of them. Formal proof occurs when a theorem demonstration is shown

Table 3
Evaluation of the research studies.

Categories	Amount of works
Without evaluation	37
Scenarios description	24
Informal discussion	17
Performance analysis	12
Formal proof	3

[19]. Performance analysis is inherent only in works with experiments [7] and, in some cases, this analysis can indicate the solution scalability [19]. Thus, the evaluation method depends on the type of the proposed solution.

Our literature review shows that research studies without deployment in real clouds are predominant and that an analysis of the works with experiments shows normally the use of private clouds. The private clouds were known platforms or infrastructures of local projects. The platforms cited are VMware vSphere, OpenNebula and OpenStack. The management of the virtual machines is done by the hypervisors and the following are mentioned: Xen, Hyper-V and KVM (Kernel-based Virtual Machine). None of these tools has been widely used.

Most of the solutions were deployed in an Infrastructure as a Service (IaaS) model, but the validation of the architecture proposed by Almorsy et al. [18] was done, in a Software as a Service (SaaS) context, with a multi-tenant application. Besides, the research studies consider a single deployment model, except the solution proposed by Silva and Geus [25] that monitors both the infrastructure and the provided service.

The lack of works involving public clouds is due to restrictions of control over the cloud infrastructures. However, Popa et al. [19] perform experiments in Microsoft Azure platform. Lastly, we highlight the limitation of details about the deployment of some works [7,24].

4. Open challenges

The systematic mapping, described in the previous section, highlights some initiatives inherent to the use of security SLAs for cloud computing and exposes the relevance of this topic. The selected papers do not treat all parts of the life cycle in SLA management and focus mainly on negotiation or operationalization aspects. There are few works that address both phases, and the relationship between these aspects is not always suitable, such as in the approach proposed by Rak et al. [29]. In this study, backup frequency and key length are parameter examples to be negotiated, but the monitoring is based on intrusion detection.

When a generic solution is proposed, it is classified in the conceptual model category, due to the absence of details (e.g., security metrics) and deployment in a cloud. The detailed works focus on a specific scenario, addressing a single security aspect or a single phase of the life cycle. Thus, the main challenge resulting from this review is the development of a solution that integrates properly the whole SLA life cycle and treats various security aspects. We identified research opportunities to enable the development of an SLA management solution. In the rest of this section, we discuss these research opportunities:

- the definition of a standard for security SLAs for clouds;
- the definition of security metrics to be measured in the SLA operationalization;
- the development of mechanisms for violation management, allowing the SLA reestablishment;
- the inclusion of a re-negotiation process, satisfying the changes of the clients' requirements;
- the identification of the limitations that unable the deployment in public clouds, proposing solutions to overcome them;
- the creation of an artifact that aids the clients during the SLA negotiation process;
- the use of mechanisms for security monitoring, avoiding the denial of the SLA violation;
- the creation of techniques to provide guarantees, through an SLA, of security aspects do not properly address in literature;
- the proper evaluation of the solutions, demonstrating the security of them;
- the elimination of the human intervention in procedures that can be automated; and
- the inclusion of de-commissioning phase in SLA management.

We highlight firstly the lack of a standard for security SLAs for clouds and this lack hampers the comparison among SLAs of the providers. CSA developed the STAR program, making viable this comparison [20]. In this program, the maturity level of the cloud providers is evaluated in accordance with the applied security controls.

In the discussion of the research questions, we presented some works that emphasize the difficulty in defining security metrics and monitor them in SLA operationalization. For example, Chaves et al. [8] present some security concerns and exemplify the security levels with metrics for backup planning. Although they introduce a monitoring architecture, they do not specify how the measurement is performed.

We highlighted also that the violation management is neglected in found studies. The violation management allows not only detect SLA violations, but also the SLA reestablishment. The SLA re-negotiation can be used to restore an SLA too.

Besides, the re-negotiation allows that an SLA can satisfy the new needs of a client. When we analyze the deployment of solutions in real clouds, we found few papers that show experiments, especially in public clouds, due to the control limitations of these infrastructures.

Chaves et al. [8] provide an overview of SLA use for security management in clouds and show some difficulties for this management. The clients should analyze their security policies and the providers' architectures. These steps are necessary to understand the clients' needs and to verify if their services could be migrated to some cloud provider. This analysis is not trivial because the clients usually specify security requirements while the providers expose security mechanisms, making it difficult to define SLA parameters and their values. Furthermore, Chaves et al. [8] emphasize the necessity of a security monitoring, resulting in the increase of the client's trust in the QoS. This is possible using secure logs or independent auditors, avoiding the tampering of the collected data and the denial of a violation. Although, there are some studies addressing the security monitoring, the found solutions focus on specifics scenarios.

Rong et al. [3] believe that the major security concern is related to the assurance of the confidentiality and integrity of the data storage in clouds. We found only seven studies that address exclusively the cloud secure storage. Thus, despite the existence of several initiatives to offer secure storage, a small number of these present a direct relationship with the SLAs [9,19,22]. We believe that the guarantee of data confidentiality in SLAs is still a challenge. Chuang et al. [22] address the data leakage, assuring with some probability that a data leakage did not happen. In their work, there is only an assumption of the probability to violate a single storage node, without any relationship with the used encryption.

In Table 3, we pointed that few solutions present a formal proof of their security. Besides the deployment of a solution in a cloud infrastructure, it is necessary to prove properly its security. In some works, the presented theorems are not demonstrated formally [19]. In our previous work [30], we use CPNs (Colored Petri Nets) to model and evaluate the solution proposed by Popa et al. [19]. Our results identify scenarios in which security violations were not detected by this solution.

The automation is an important aspect of SLA management, facilitating the SLA negotiation [10,11]. The automation also provides agility in monitoring and allows an immediate reaction when occurring an SLA violation [26]. However, in the solution proposed by Djemame et al. [23], experts perform the measurement, requiring a manual intervention in tasks that should be automatic. Another fundamental aspect is the adequacy of the solutions to cloud computing environments. Only few studies evaluate, for example, the scalability of the proposed solutions. A cloud infrastructure is shared with several users, requiring then the development of solutions that promote and ensure the resources' isolation [21]. Thus, the viability of a solution for SLA management has not always been proved in analyzed papers.

Lastly, de-commissioning was a neglected phase in the selected research studies and a single study addresses this aspect [13]. In this study, the system CPOD (Cloud-Proof of Deletion) is proposed to ensure the destruction of the client data, when an SLA is terminated. The authors also guarantee the backup removal and evaluate the solution performance. On the other hand, it is necessary to provide others guarantees, allowing the portability of the client services to another provider, or the backup of the client data and applications.

Although there are solutions for services migrations, using for example OCCI (Open Cloud Computing Interface), some barriers should be overcome, and the end of an SLA can occur due to an eventual bankruptcy of the provider. For example, the Nivanix provider declared bankruptcy on September 2013 and informed his clients that their data were only available until the end of the month.[14] However, it is possible that a provider does not have financial resources to allow the backup of the clients' data. Thus, de-commissioning is a fundamental aspect of a security SLA solution.

5. Conclusions and future work

Security is one of the users' concerns when using cloud computing services. This paper described a systematic mapping of the literature about research that uses the SLA to mitigate this concern. Firstly, an overview of the existing works was presented here, with a classification of the selected studies. This mapping revealed that the generic studies do not expose the viability of their solutions, and the concrete solutions focus on a specific security aspect and on a single phase of the SLA life cycle.

Next, we discussed the research questions, highlighting the aspects that must be considered during the SLA negotiation and operationalization. The studies about SLA negotiation normally focus on selection of the providers or security services. Besides of the definition of SLA security parameters, the negotiation protocol and the language for SLA specification was underlined as the key elements to compose this phase. In relation to the operationalization phase, the main activity is the monitoring of the negotiated parameters to verify the QoS of the provided service. Audit mechanisms have been used to prove this QoS and attest that no SLA violation happened.

The analyzed works show the relevance of this topic and at the end of this paper, we collected challenges to underline the research opportunities that should be treated in future work. It is necessary to develop a robust and autonomic solution to SLA for cloud security, managing all life cycle. The definition of suitable SLA parameters and their metrics is important to allow the integration between the negotiation and operationalization phases. The security monitoring is essential to increase the trust in the cloud environment, and the violation management and SLA re-negotiation are activities that cannot be neglected.

[14] http://en.wikipedia.org/wiki/Nirvanix.

Thus, the definition of security SLA for clouds is an open topic and this review summarizes the knowledge to guide the future work about this theme. The review, presented here, does not have the intention to exhaust all the literature about this topic, and it can be expanded with other studies about security measurement that could be suitable for the cloud computing scenario.

Acknowledgment

This work is partially supported by the STIC-AmSud project SLA4Cloud. Carlos André Batista de Carvalho was also supported by CAPES/FAPEPI Doctoral Scholarship, and Rossana Maria de Castro Andrade has a researcher scholarship (DT Level 2), sponsored by CNPq (Brazil).

[1] Casola V, Benedictis AD, Rak M. On the adoption of security slas in the cloud. In: Accountability and security in the cloud. Springer Berlin Heidelberg; 2015. p. 45–62.
[2] Luna J, Suri N, Iorga M, Karmel A. Leveraging the potential of cloud security service-level agreements through standards. IEEE Cloud Comput Mag 2015;2(3):32–40.
[3] Rong C, Nguyen ST, Jaatun MG. Beyond lightning: a survey on security challenges in cloud computing. Comput Electr Eng 2013;39(1):47–54.
[4] Bose S, Pasala A, Ramanujam A D, Murthy S, Malaiyandisamy G. Sla management in cloud computing: a service provider's perspective. In: Cloud computing: principles and paradigms. John Wiley & Sons; 2011. p. 413–36.
[5] Faniyi F, Bahsoon R. A systematic review of service level management in the cloud. ACM Comput Surv 2015;48(3) 43:1–43:27.
[6] Bernsmed K, Jaatun MG, Meland PH, Undheim A. Security slas for federated cloud services. In: Proceedings of the 6th international conference on availability, reliability and security, ARES'11; 2011. p. 202–9.
[7] Park K-W, Han J, Chung J, Park KH. Themis: a mutually verifiable billing system for the cloud computing environment. IEEE Trans Serv Comput 2013;6(3):300–13.
[8] de Chaves SA, Westphall CB, Lamin FR. Sla perspective in security management for cloud computing. In: Proceedings of the 6th international conference on networking and services, ICNS'10; 2010. p. 212–17.
[9] Albeshri A, Boyd C, Gonzalez Nieto J. Geoproof: proofs of geographic location for cloud computing environment. In: Proceedings of the 32nd IEEE international conference on distributed computing systems workshops, ICDCSW'12; 2012. p. 506–14.
[10] Guesmi A, Clemente P. Access control and security properties requirements specification for clouds' seclas. In: Proceedings of the 2013 IEEE 5th international conference on cloud computing technology and science, CloudCom'13, 1; 2013. p. 723–9.
[11] Meland PH, Bernsmed K, Jaatun MG, Castejón HN, Undheim A. Expressing cloud security requirements for slas in deontic contract languages for cloud brokers. Int J Cloud Comput 2014;3(1):69–93.
[12] Top Threats Working Group. The notorious nine: cloud computing top threats in 2013. Tech. Rep.. Cloud Security Aliance; 2013.
[13] Vanitha M, Kavitha C. Secured data destruction in cloud based multi-tenant database architecture. In: International conference on computer communication and informatics; 2014. p. 1–6.
[14] Manuel P. A trust model of cloud computing based on quality of service. Ann Oper Res 2013:1–12.
[15] Hussain M, Al-Mourad MB. Effective third party auditing in cloud computing. In: Proceedings of the 2014 IEEE 28th international conference on advanced information networking and applications workshops, WAINA'14; 2014. p. 91–5.
[16] Ficco M, Rak M. Intrusion tolerance as a service: a sla-based solution. In: Proceedings of the 2nd international conference on cloud computing and services science, CLOSER'12; 2012. p. 375–84.
[17] Binu V, Gangadhar ND. A cloud computing service level agreement framework with negotiation and secure monitoring. In: IEEE international conference on cloud computing in emerging markets (CCEM); 2014. p. 1–8.
[18] Almorsy M, Grundy J, Ibrahim AS. Collaboration-based cloud computing security management framework. In: Proceedings of the IEEE 4th international conference on cloud computing, CLOUD'11; 2011. p. 364–71.
[19] Popa RA, Lorch JR, Molnar D, Wang HJ, Zhuang L. Enabling security in cloud storage slas with cloudproof. In: Proceedings of the 2011 USENIX conference on USENIX annual technical conference, USENIXATC'11; 2011.
[20] Zhengwei J, Ran D, Zhigang L, Xihong W, Baoxu L. A meta-synthesis approach for cloud service provider selection based on secsla. In: Proceedings of the 2013 15th international conference on computational and information sciences, ICCIS'13; 2013. p. 1356–60.
[21] Raj H, Nathuji R, Singh A, England P. Resource management for isolation enhanced cloud services. In: Proceedings of the 2009 ACM workshop on cloud computing security, CCSW'09; 2009. p. 77–84.
[22] Chuang I-H, Huang Y-T, Su W-T, Lin T-S, Kuo Y-H. S4: an sla-aware short-secret-sharing cloud storage system. In: Ubiquitous and future networks (ICUFN), 2015 seventh international conference on; 2015. p. 401–6.
[23] Djemame K, Barnitzke B, Corrales M, Kiran M, Jiang M, Armstrong D, et al. Legal issues in clouds: towards a risk inventory. Philos Trans R Soc A 2013;371(1983).
[24] Chauhan NS, Saxena A, Murthy J. An approach to measure security of cloud hosted application. In: Proceedings of the 2013 IEEE international conference on cloud computing in emerging markets, CCEM'13; 2013. p. 1–6.
[25] da Silva CA, de Geus PL. An approach to security-sla in cloud computing environment. In: IEEE Latin-America conference on communications; 2014. p. 1–6.
[26] Doelitzscher F, Reich C, Knahl M, Clarke N. An autonomous agent based incident detection system for cloud environments. In: Proceedings of the 2011 IEEE 3rd international conference on cloud computing technology and science, CloudCom'11; 2011. p. 197–204.
[27] Casalicchio E, Silvestri L. An inter-cloud outsourcing model to scale performance, availability and security. In: Proceedings of the 2012 IEEE/ACM 5th international conference on utility and cloud computing, UCC'12; 2012. p. 151–8.
[28] Petcu D, Craciun C. Towards a security sla-based cloud monitoring service. In: Proceedings of the 4nd international conference on cloud computing and services science, CLOSER'14; 2014. p. 598–603.
[29] Rak M, Suri N, Luna J, Petcu D, Casola V, Villano U. Security as a service using an sla-based approach via specs. In: Proceedings of the 2013 IEEE 5th international conference on cloud computing technology and science, CloudCom'13, 2; 2013. p. 1–6.
[30] de Carvalho CAB, de Castro Andrade RM, de Castro MF, Agoulmine N. Modelagem e detecção de falhas em soluções para armazenamento seguro em nuvens usando redes de petri coloridas: um estudo de caso. In: Proceedings of the 34th Brazilian symposium on computer networks and distributed systems (SBRC) - 14th cloud computing and applications workshop (WCGA); 2016. p. 17–30. *Original in Portuguese*