
SERVICE LEVEL AGREEMENTS AND SECURITY SLA: A COMPREHENSIVE SURVEY

Serena Nicolazzo

Department of Computer Science,
University of Milan, Italy
serena.nicolazzo@unimi.it

Antonino Nocera

Department of Electrical, Computer and
Biomedical Engineering,
University of Pavia, Italy
antonino.nocera@unipv.it

Witold Pedrycz

Department of Electrical and Computer Engineering,
University of Alberta, Edmonton, AB T6G 2R3, Canada and
Systems Research Institute, Polish Academy of Sciences 00-901 Warsaw, Poland and
Research Center of Performance and Productivity Analysis, Istinye University Istanbul, Türkiye
wpedrycz@ualberta.ca

ABSTRACT

A Service Level Agreement (SLA) is a formal contract between a service provider and a consumer, representing a crucial instrument to define, manage, and maintain relationships between these two parties. The SLA's ability to define the Quality of Service (QoS) expectations, standards, and accountability helps to deliver high-quality services and increase client confidence in disparate application domains, such as Cloud computing and the Internet of Things. An open research direction in this context is related to the possible integration of new metrics to address the security and privacy aspects of services, thus providing protection of sensitive information, mitigating risks, and building trust. This survey paper identifies state of the art covering concepts, approaches, and open problems of SLA management with a distinctive and original focus on the recent development of Security SLA (SecSLA). It contributes by carrying out a comprehensive review and covering the gap between the analyses proposed in existing surveys and the most recent literature on this topic, spanning from 2017 to 2023. Moreover, it proposes a novel classification criterium to organize the analysis based on SLA life cycle phases. This original point of view can help both academics and industrial practitioners to understand and properly locate existing contributions in the advancement of the different aspects of SLA technology. The present work highlights the importance of the covered topics and the need for new research improvements to tackle present and demanding challenges.

Keywords Service Level Agreement, SLA Management, Security Service Level Agreement, Privacy Level Agreement, SLA, SecSLA, PLA, Cloud Computing, IoT.

1 Introduction

Establishing clear and shared rules between consumers and providers to regulate IT service provisioning is a key factor for guaranteeing the expected quality of service and increasing parties' protection in case of disputes or disagreements. This is even more true in modern Cloud computing and Internet of Things (IoT) environments characterized by high dynamicity and the intrinsic heterogeneity of their components.

To tackle this problem, Service Level Agreements (SLAs, for short) have been proposed as an effective method to manage and guarantee the promised Quality of Service (QoS), accurate reporting on service usage, and runtime adaptation for evolving requirements.

An SLA is a formal and legally binding contract or agreement defining the terms and performance metrics that the service provider commits to delivering and the customer expects to receive. Therefore, from the providers' side, an SLA ensures that they can avoid penalties if the appropriate levels of agreement have been respected during the service provisioning, and, at the same time, providers can strengthen their credibility if the given conditions have been always met. On the other hand, also customers can benefit from these contracts because they can be assured that the favored service will follow the chosen terms [1].

Especially in the above-cited Cloud and IoT contexts, SLA management gives rise to several challenges. These can be related to the lack of transparency on the actual performance of the services (which can vary also for external conditions), little control over infrastructures, multi-tenancy heterogeneous hardware, lack of standardization and specific regulatory requirements from different industries and regions, and, finally, the increasing number of connected devices that gives rise to scalability problems[2, 3]. Still in this context, a major challenge is related to the vulnerability to security and privacy threats, which may lead to information disclosure and service unavailability. On the other hand, attacks on infrastructures and devices directly impact the goals of SLAs [4]. While security has long been considered a potential element of SLAs [5], establishing measurable and commonly agreed-upon security metrics has always been considered a hard task for researchers and practitioners. Consequently, identifying approaches to effectively manage security throughout all the phases of the SLA life cycle requires a systematic review of existing contributions and additional research efforts in this direction [6].

The main goal of this survey paper is to carry out a detailed and critical investigation of the existing research on the management of SLAs. To do so, we retrieve relevant studies focusing on various aspects of SLA management and propose a classification based on the SLA life cycle discussed in the European Commission Report [1]. Starting from this, by analyzing the contributions available in the literature, we can identify three main categories, covering SLA modeling, SLA negotiation, and SLA monitoring and violation, which we can use to organize our systematic analysis. As an additional important contribution, in our proposal, we focus on approaches leveraging Security Service Level Agreements (SecSLA, hereafter), which attempt to integrate security metrics into SLAs. Moreover, still, in this context, we consider Privacy Level Agreements (PLAs), which are a subcategory of SecSLAs specifically dealing with notions related to privacy protection practices. Then, we evaluate the existing literature maturity level and find commonalities and research gaps also drawing possible future directions and open issues for the research community.

The contribution of this study can be classified into the following four main folds:

- we identify the most prominent and recent studies related to SLA and Security SLA.
- We provide a comprehensive analysis of the main basic concepts related to SLA, such as SLA definition, life cycle, and language specifications.
- We undertake a complete examination of the identified approaches and organize our analysis based on the SLA life cycle phases.
- We thoroughly examine open issues, challenges, and future trends of SLA and SecSLA approaches.

We believe that this paper can contribute to the academic discourse and industrial progress in identifying the open challenges in this context and providing a clear and updated picture of the SLA and SecSLA landscape. Although SLA and SecSLA play a crucial role in defining shared rules and security metrics for services at design time, nevertheless, a comprehensive survey on recent advancements in SLA and SecSLA is missing in the current scientific literature. Moreover, by organizing our analysis using the SLA life cycle phases to group related proposals, this survey paper can help academics and industrial practitioners to understand and properly locate the contributions, available in the recent literature, to the different aspects of the SLA technology.

The remainder of this paper is organized as follows. Section 2 focuses on the methodology employed to conduct this work, whereas Section 3 discusses the articles related to our survey. In Section 4, we overview the main concepts related to Service Level Agreements, namely SLA definition, characteristics, actors, life cycle, and classical language specifications. Section 5 reviews the literature relying on our proposed classification method focusing on the SLA life cycle aspects of modeling, negotiation, monitoring, and violation. Section 6 examines the existing scientific contributions from a security and privacy perspective describing works dealing with SecSLAs. Section 7 delves into the open problems and future research directions. Finally, Section 8 provides a summary of the present survey, offers some perspective and opportunities, and concludes this work.

2 Methodology

In this paper, we conduct a survey study following the guidelines drawn in [7] to identify published research results that are relevant to the research area of interest. We accomplish a comprehensive literature review process, following these

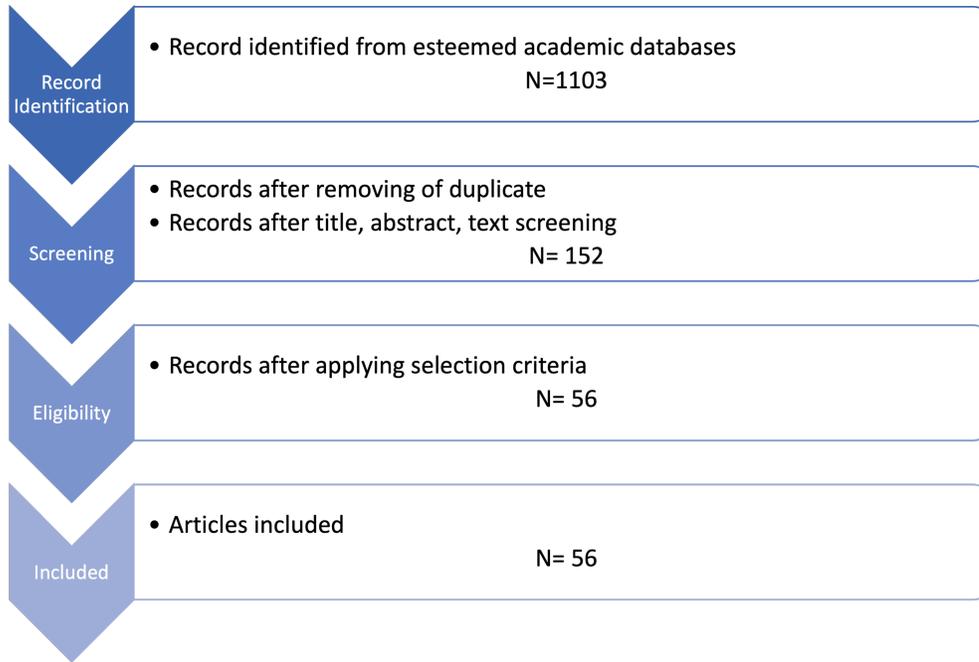


Figure 1: PRISMA flowchart for paper selection process

steps: (i) defining clear search objectives, (ii) identifying relevant literature from journals and conference proceedings leveraging search engines and driven by a well-defined search strategy, and (iii) applying selection criteria to filter the articles during this iterative process. Figure 1 shows the PRISMA flow diagram, providing a visual representation of the above-described screening process. The diagram highlights the count of research works identified, excluded, and included.

2.1 Search strategy

To gather relevant research focusing on SLA, we designed a search strategy to align with our research objectives. We meticulously performed searches through esteemed academic databases, such as (i) IEEE Xplore Digital Library [8], (ii) Scopus [9], (iii) Google Scholar [10], and (iv) ACM Digital Library [11]. The search scope comprises a broad range of publication years from 2017 to 2023, ensuring a well-rounded coverage of recent research in the field. Furthermore, we developed the search terms to identify relevant investigations and employ a combination of specific keywords and phrases to encompass various aspects of SLA. The primary search terms include “Service Level Agreement”, and “SLA”. In conjunction with the primary terms we used additional keywords such as “SecSla”, “PLA”, “SLA management”, “IoT”, “Web Service”, and “Cloud Computing”.

Starting from these terms, we formulated the following search string:

(“Service Level Agreement” OR “SLA” OR “SLA Management”)
 AND
 (“Security Service Level Agreement” OR “SecSLA” OR “Security SLA” OR
 “Privacy Service Level Agreement” OR “PLA”)
 AND
 (“Internet of Things” OR “IoT” OR “Industrial Internet of Things” OR
 “Cloud” OR “Cloud Computing” OR “Web Service”)

2.2 Selection criteria

In this section, we list the selection criteria we used to decide whether a scientific work, identified through the above-described search query, is appropriate for our study and reaches enough quality to be included in this survey. A paper is eligible for inclusion in the present work if it satisfies at least one of the inclusion criteria and none of the exclusion criteria applies. At the end of this screening, 56 papers were finally selected.

2.2.1 Inclusion Criteria

To evaluate the relevance of a paper and include it in our survey, we observed the following criteria:

- the corresponding author or the supervisor’s importance in the field under analysis;
- the importance of the venue (journal or conference) where the paper has been published (we consider Scimago [12] and Core.edu [13] as ranking Web sites for journals and conferences, respectively).

2.2.2 Exclusion Criteria

After the inclusion, the exclusion process is followed. A paper is excluded if one of the following criteria is met:

- the paper is not written in English;
- the paper is not peer-reviewed;
- the paper’s year of publication is earlier than 2017;
- the paper is not specifically focused on SLA nor contributes to this context;
- the paper lacks relevance, it is an incremental refinement of an earlier proposed approach, there is a duplicate publication, or there is a more recent and cited version of the work published in a prestigious venue.

2.2.3 Selection Process

We used a two-step selection process to identify relevant publications in our study as shown in Figure 1. In the first step, we initially collected 1,103 possibly relevant publications, specifically: 290 from IEEE Xplore Digital Library, 445 from Scopus, 124 from Google Scholar, and 264 from ACM Digital Library. Starting from this set, we deleted duplicates and performed a first screening of the abstract and text of the articles. Moreover, we also analyzed the bibliographies of the selected articles to identify possible additional interesting contributions. This step led to 152 publications left. Next, we applied the inclusion and exclusion criteria defined before to classify papers relevant to our survey and not relevant ones. The relevant publications were sorted according to the following categories: SLA Definition, SLA Modeling, SLA Negotiation, SLA Monitoring and Violation, and Security and Privacy SLA (see Section 4.2). This last step in the selection process shortlisted 56 publications out of 152 identified studies. Therefore, this survey’s final list of studies consists of 56 publications.

3 Related Work

In this section, we provide an overview of the existing research literature in the field of SLA, SLA management, and Security SLA.

The survey paper presented in [2] mainly focuses on the definition and SLA modeling for Cloud services in IoT. They analyze 44 publications between 2017 and 2018. The classification scheme used to group the papers refers to the following groups: *(i)* ontology, *(ii)* languages, *(iii)* frameworks and methodologies, *(v)* templates and *(vi)* matching of services and consumer needs. The papers [14, 15] deal with the management of SLAs in IoT applications. In particular, [14] identifies 328 studies and categorizes them into seven technical classifications of the SLA life cycle. Instead, the work of Papadopoulos et al. [15] conducts a systematic mapping study to allow for a concise understanding of the status of SLA management in industrial IoT analyzing works between 2012 and 2016.

Several works focus only on a specific aspect of the SLA life cycle [16, 17, 18]. For instance, the survey article in [16] focuses particularly on the SLA negotiation phase in Cloud computing studying a few research contributions from 2009 to 2017. Instead, the work [17] examines 23 papers related to monitoring and prediction techniques for the efficient usage of IaaS Cloud resources. A recent contribution [18] focuses on approaches based on Blockchain technology. This survey analyzes papers, published over the period from 2018 to 2020, which employ this technology to provide trust between consumers and service providers based on SLA violations and compensation enforcements.

The objective of the surveys proposed in [19, 20] is to examine Cloud service computing and SLA. In particular, [19] discusses briefly Cloud SLAs, their issues, and developmental challenges providing also a description of the major commercial Cloud providers. The authors of [20], instead, document techniques for scheduling and resource allocation in the Cloud.

A recent survey paper from Sharma et al. [21] deals with intent-driven service management (IDSMS) systems. In this context, intent is defined as a declarative expression representing what a user wants to achieve instead of how it

Table 1: Survey papers related to our work

Paper	Literature timeline	Paper Type	SLA Definition	SLA Modeling	SLA Negotiation	SLA Monitoring and Violation	SecSLA and PLA	Domain
He and Sun [16]	2009-2017	Survey	-	-	✓	-	-	Cloud
Papadopoulos et al. [15]	2012- 2016	Systematic Review	✓	✓	✓	✓	-	Industrial IoT
Girs et al. [2]	2017-2018	Survey	✓	✓	-	-	-	Cloud-based IoT
Mubeen et al. [14]	2009-2016	Survey	✓	✓	✓	✓	-	Cloud-based IoT
Odun-Ayo et al. [19]	2009-2016	Survey	✓	-	-	-	-	Cloud
Odun-Ayo et al. [20]	2008-2018	Survey	✓	-	-	-	-	Cloud
Sharma et al. [21]	2016-2022	Survey	✓	-	-	-	-	IDSMS
Nugraha and Martin [22]	1999-2017	Survey	-	-	-	-	✓	-
De Carvalho [23]	2009-2015	Systematic Review	-	-	-	-	✓	Cloud
Prasad and Bhavsar [17]	2000-2017	Survey	-	-	-	✓	-	IaaS Cloud
Hamdi et al. [18]	2018–2020	Survey	-	-	-	✓	-	-
Our Survey	2017-2023	Survey	✓	✓	✓	✓	✓	IoT, Cloud, Cloud-based IoT, Web Services

should be achieved. The authors focus on works related to SLA management, specifying SLAs as intents. Moreover, a taxonomy is proposed and used to compare the analyzed techniques in IDSMS systems.

A few works analyze SecSLA [22, 23] with a focus on the open problems and existing solutions when integrating security properties into SLA contexts and, hence, providing a review of the literature on trustworthy SLAs.

In comparison with the existing survey articles, analyzed in this section, our paper presents a complete discussion of publications produced in a very recent period (i.e., from 2018 to 2023) of all the phases of SLA Management (i.e., definition, modeling, negotiation, monitoring, and violation). Moreover, unlike earlier endeavors, our work delves into the security and privacy aspects of SLA, providing an investigation of recent analyses dealing with this perspective. This distinctive focus characterizes our paper concerning the existing body of literature, highlighting its originality and potential impact on the advancement of knowledge in the field.

Table 1 provides a summary analysis of the contributions of the existing related survey papers compared to ours. In particular, this table illustrates the period of the analyzed publication, its type (i.e., survey paper or systematic review), the different phases of the SLA life cycle considered in the paper, the focus on security or privacy SLAs, and the domain of application. Observe that, we refer to systematic reviews if the work provides only a synthesis of the analyzed results about the SLA topic, privileging numerics but not descriptions.

4 Background

In this section, we provide the necessary background for this survey paper. In particular, we define what is an SLA and describe its main components, all the phases related to its life cycle, the defined language specifications, and the categorization employed throughout this work. Table 2 summarizes the acronyms used in this paper.

4.1 SLA Definition

A Service Level Agreement (SLA) is a formal contract between a service provider and a customer that outlines the level of service the customer can expect. The European Commission Report on recent European and national projects covering Cloud computing SLAs [1] gives a formal definition of such a recommendation:

Table 2: Summary of the acronyms used in the paper.

Symbol	Description
IDSM	Intent-Driven Service Management
IMS	IP Multimedia Subsystem
IoT	Internet of Thing
ML	Machine Learning
PLA	Privacy Service Level Agreement
QoS	Quality of Service
RL	Reinforcement Learning
SecSLA	Security Service Level Agreement
SLA	Service Level Agreement
SLI	Service Level Indicator
SLM	Service Level Management
SLO	Service Level Objective
WSDL	Web Services Description Language
WSLA	Web Service Level Agreement
WSN	Wireless Sensor Network

A Service Level Agreement (SLA) is a formal, negotiated document that defines (or attempts to define) in quantitative (and perhaps qualitative) terms the service being offered to a Customer. Any metrics included in an SLA should be capable of being measured on a regular basis and the SLA should be recorded by whom.

According to the previous definition, the purpose of an SLA is to define the terms, conditions, and expectations for the service being provided, as well as the responsibilities of both parties [24, 15]. Since SLAs provide a clear and measurable framework for understanding and managing service delivery, they represent key factors in Service Level Management (SLM), which is the process that focuses on managing and improving the quality of services provided by an IT service provider.

Specifically, in [15] several characteristics defining a proper SLA are listed, namely:

- **Attainability** is the possibility of meeting the desired level of service;
- **Meaningfulness** is a property defining that all SLA parts must be relevant to the agreement;
- **Measurability** defines that the level of service provisioning should be measurable in an impartial way;
- **Controllability** specifies that the factors impacting the SLA must be under the service provider’s control;
- **Understandability** means that both parties must understand the concepts and quantities of the SLA;
- **Affordability** is a property determining that the SLA should be cost-effective;
- **Mutual acceptability** is related to the definition of the SLA that should be the result of the negotiation between parties.

As an “agreement”, an SLA includes a set of different features regarding the provisioning of the service. These refer to the agreed Quality of Service (QoS, hereafter) declined through different terms, the Service Level Objectives (SLOs), the responsibilities and obligations of the parties, as well as the penalties in cases of non-compliance to the agreed terms. Specifically, the following components must be present in an SLA [25, 2]:

- **Service Name and Description** provide the name and description of each offered service and the main objective of the whole SLA.
- **Parties** describe an individual or group of entities involved in the contract and their roles (i.e., service provider and consumer). A party could be a private, commercial, or public entity.
- **Validity Period** defining the period covered by the SLA.
- **Scope** of the agreement.
- **Restrictions**, defining the steps to be taken to provide the service.
- **Service Level Indicator (SLI)** is a parameter or a metric associated with a service able to specify a certain quantitative or qualitative level of service. Examples include availability, latency, response time, jitter, scalability, processing capacity, memory, storage, and so on.



Figure 2: SLA life cycle

- **Service Level Objective (SLO)** representing a threshold or a value on an SLI or a metric.
- **Penalties** defining what happens in case the service provider is unable to meet the objectives in the SLA. Specifically, the penalty parameter refers to the fee that the service provider must pay to the service consumer if the SLO specified on an associated SLI is not met.
- **Optional services** which are not mandatory for the user.
- **Exclusion** parameters are elements specifying what is not covered in the SLA.
- **Administration** describing the processes created in the SLA to meet and measure its objectives and defines organizational responsibility for the monitoring of those processes.

Moreover, according to the different perspectives an SLA may have and the services offered, two main SLA modalities exist [26]. The former type is *Service-Based SLA*, which refers to non-negotiable and ready-to-sign SLAs available for all consumers. This is the common type of SLA in Clouds, implying that the service agreements are the same across all customers. The latter is *Customer-Based SLA*, which has negotiable terms and is agreed upon with individuals or groups to adapt the services to their needs. Although more flexible, this modality is significantly more complex and less used.

4.2 SLA Life cycle

The SLA life cycle meta-model was first discussed in the European Commission Report [1]. As shown in Figure 2 it captures the main phases, structures, processes, and entity interactions in the SLA life cycle.

The six main phases of the SLA life cycle include:

- **Service Use.** This phase refers to the SLA definition. Before the services can be provided to the consumer, both the provider and the consumer must agree on the terms of the agreement, such as metrics, level, quality, price, and penalties.
- **Service Modeling.** This phase deals with the modeling of the service, relationships, dependencies within the service components, and information regarding the service provision. The outcome of the process could be an artifact or document (in a standard modeling language, such as XML), which includes all the parameters affecting the service execution, usage, and delivery.

Table 3: Mapping between categorization used throughout this paper and the different stages of the SLA life cycle

SLA life cycle Stage	Our Categorization Strategy
1. Service Use	SLA Definition (see Section 4.1)
2. Service Modeling	SLA Modeling (see Section 5.1)
3. SLA Template Definition	SLA Modeling (see Section 5.1)
4. SLA Instantiation and Management	SLA Negotiation (see Section 5.2)
5. SLA Enforcement	SLA Monitoring and Violation (see Section 5.3)
6. SLA Conclusion	SLA Monitoring and Violation (see Section 5.3)

- **SLA Template Definition.** In this phase, SLA templates are created and other related information is captured.
- **SLA Instantiation and Management.** This phase deals with the mechanisms for discovering providers for specific services and dynamic negotiation between participating entities.
- **SLA Enforcement.** This phase retains the quality parameters (agreed in signed SLAs). All providers exploit monitoring mechanisms and SLA violation detection mechanisms to trigger corrective actions.
- **SLA Conclusion.** This phase handles the termination of the SLA, which can happen for various reasons such as the service delivery has been successfully concluded, the SLA validity period has expired, or an SLA violation has occurred.

Starting from the above SLA life cycle and the technical classification used in [14], we identify a criterium to categorize the analyzed literature and group the different studies in the rest of this investigation. Specifically, we leverage the following classification categories:

- **SLA Modeling.** This category comprises frameworks, templates, and modeling languages to model SLA solutions that have been proposed in the recent literature. This category can be mapped to the SLA Modeling and SLA Template Definition stages of the SLA life cycle.
- **SLA Negotiation.** This category includes papers focusing on group framework to create non-negotiable, negotiable, and re-negotiable SLAs. This group concerns the SLA Instantiation and Management phases of the SLA life cycle.
- **SLA Monitoring and Violation.** Approaches to check and evaluate the expected level of service are grouped in this category. Moreover, papers on the economic penalties derived from possible SLA violations are also analyzed. This category can be mapped to the SLA enforcement and SLA Conclusion stages of the SLA life cycle.

Table 3 shows the mapping between the categorization strategy used throughout this article and the different stages of the SLA life cycle. Observe that, not all the SLA life cycle categories are used in this paper to categorize the literature research. In particular, the Service Use stage has been mainly discussed in very old research proposals and, hence, we included them in Section 4.1, where we defined background concepts related to SLA and its characteristics.

4.3 SLA Language Specifications

This section discusses the state-of-the-art research on SLA specification languages. The procedure through which different SLAs are automatically described, provisioned, and observed is quite recent. Before it, SLA contracts were mostly written using natural expressions, and the examination of compliance was done manually [27]. The current most prominent industrial approaches for SLA language specification are: WSLA, WS-Agreement, SLA*, CSLA, SLAC, RBSLA, and SLA-IoT [28].

WSLA. IBM published the Web Service Level Agreement (WSLA), which provides a specification for the definition and monitoring of SLAs within a Web Service environment [29]. A WSLA provides a runtime architecture and a language for SLA specification for Web services documents. It describes the assertions of a service provider concerning the service including (i) the agreed parameters (e.g., response time and throughput) derived from business metrics and (ii) the measures to be taken in case of failure to meet the service guarantees (for instance, a notification of the service customer). As shown in Figure 3, the service provider’s assertions are based on a detailed definition of both basic and composite service metrics. Underlying, these are derived from low-level metrics related to the resources residing in the service provider tier.

In addition, a WSLA also expresses the actor included in the architecture, namely the monitoring party, third parties that contribute to the measurement of metrics, and the management of deviations of service guarantees. The different

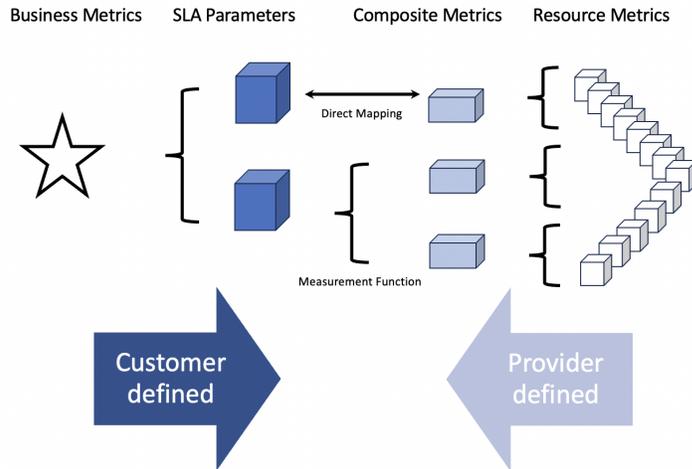


Figure 3: WSLA terminology and main components

parties define a proprietary implementation policy for a service that has to be translated into system-level configuration information, thus creating an independent deployment function that interprets the WSLA and takes appropriate actions for each party.

The WSLA language is based on XML and defined as an XML schema. The language is extensible to include: (i) specific types of operation descriptions (e.g., using WSDL to describe a Web services operation), (ii) measurement directive types for specific systems, (iii) special functions to compose aggregate metrics, and (iv) predicates to evaluate specific metrics.

Observe that, a WSLA defines the agreed performance characteristics and how to evaluate and measure them. Instead, a service description, such as the Web Services Description Language (WSDL), describes the service interface relationship between a service and its application.

WS-Agreement. WS-Agreement is another XML-based Web Service SLA specification defined by Open Grid Forum (OGF) [30]. The specification is composed of (i) two schemas for specifying both the agreement and the agreement template, and (ii) a set of port types and operations for managing the different phases of the agreement life cycle (including creation, expiration, and monitoring of agreement states). WS-Agreement contains more information about the service functional's properties than WSLA and it allows for the extension of new domain-specific elements.

SLA*. An abstract SLA syntax named SLA* is proposed in [31] to automate the Cloud SLA life cycle. SLA* is a domain-independent syntax for machine-readable SLAs and SLA templates. This solution promotes the formalization of a SLA in any language and for any service, by eliminating the limitation of XML. This model was designed as part of the FP7 ICT Integrated Project SLA@SOI¹, and has been used in several industrial use-cases, such as Enterprise IT, live-media streaming and health-care provision.

CSLA. Cloud Service Level Agreement (CSLA) [32] is an SLA language, based on WSLA and SLA*, designed to express both SLA specifications and address SLA violations in the context of Cloud services [33]. Besides the standard formal definition of contracts comprising validity, parties, services definition, and guarantees, CSLA is enriched with features introducing language support for Cloud elasticity management (i.e., QoS/functionality degradation and an advanced penalty model).

SLAC. Like SLA* and CSLA, Service-Level-Agreement for Clouds (SLAC) [34] is a domain-specific language that defines SLAs specifically devised for the Cloud computing domain. It is inspired by the WS-Agreement and shares many features with the definition and structure of this language. The metrics available in the language are pre-defined in light of the requirements of the Cloud domain. The set of characteristics of the SLAC language, such as multiparty, group definition, and specification of the involved parties on each term, enables the definition of SLAs including a broker (i.e., an agent in charge of SLA negotiation). The semantics of the evaluation of an SLA is formulated as a Constraint Satisfaction Problem (CSP) and is intended to verify the agreement consistency and whether the characteristics of the service are within the established values.

¹<https://xlab.si/research/finished-projects/slasoi/>

RBSLA. Rule-based Service Level Agreement [35] follows a knowledge-based approach and uses RuleML [36] to specify a SLA. This formal-logical and rule-based approach provides a means to describe complex contract structures as modular rule sets, which can be collaboratively maintained, interchanged automatically, executed, and enforced by a rule engine.

SLA-IoT [37] is a recent end-to-end SLA specification language designed for the Internet of Things. It presents a new layered syntax for specifying SLA for IoT devices and their connections. A contract is composed of the classical elements such as parties, SLOs, workflow activities, services, and infrastructure resources; however, although this language allows for a more precise definition of the user’s requirements, it does not specify the penalties, devices, and user preferences.

5 Service Level Agreement

This section aims to survey the current solutions for SLA management. We grouped the papers according to our classification criterium (see Section 4.2), which is focused on the SLA life cycle. In particular, to organize our literature analysis, we considered four main topics: SLA modeling, negotiation, monitoring, and violation phases.

5.1 SLA Modeling

This category includes recently published works focusing on the definition of ontologies, templates, and languages to model SLAs.

In the context of SLA, ontology refers to a method of providing a taxonomy, that is a formal, syntactic, and semantic description model of concepts, properties, and relationships between concepts for SLA content [2]. Several studies have been focused on the definition and application of ontologies for SLA [38, 39, 40]. The proposal of [38] introduces an extension to the Linked USDL family of ontologies called Linked USDL Agreement, a semantic model to specify, manage, and share SLA descriptions on the Web. It relies on Linked Data principles [41] to share and interlink service agreements over the Web. Moreover, it exploits IDEAS, a software simulation framework-based tool, to support or evaluate the presented methods. This software provides a generic online development environment for domain-specific languages (DSL). Both the contributions presented in [40] and [39] rely on the Ontology Web Language (OWL)² to describe classes, constraints, and properties of an SLA. Their approach provides a system to calculate service price, penalty amount, and violation number, and to verify the SLA validity by defining its termination terms. The main difference is that the system in [40] specifically focuses on SLA monitoring to prove possible violations.

Several publications, rather than designing an ontology to define and model SLAs, mainly delve into presenting a new language, a language extension, or a grammar to accomplish SLA modeling [42, 43, 44, 3, 45, 26]. For instance, the authors of [42, 45, 26] focus on SLA modeling for Web Services and the Cloud. As a matter of fact, the proposal of [42] introduces the *ysla* language and engine. This language, based on YAML, defines novel constructs for configurable and reusable building blocks (namely “Templates” and “Scopes”), allowing the identification of the semantic categorizations of observation data together with metrics parameterizations. Moreover, a prototypical implementation, called *ysla* Engine, is illustrated in a multi-client, multi-provider environment. Instead, in [45] Scoca et al., define a formal language for modeling the interaction of offers and requests. They rely on dSLAC [46], a language that can be used for specifying smart contracts in the Cloud domain, and provide evidence that such contracts have clear advantages. Analogously, the work in [26] introduces a novel SLA definition language, called SLAC, specifically devised for Cloud systems as a formalism to support the whole SLA life cycle. It relies on a mechanism for dealing with the dynamicity of SLA terms, and to allow the elasticity of Cloud services and guarantee flexibility to the involved parties. SLAC supports multiple parties and all the roles in the Cloud service provision, it permits dynamic service level modifications according to pre-defined conditions and is equipped with a set of software tools supporting SLA management. A limitation of this approach is that it does not allow for the specification of device and user preferences.

Instead, the authors of [43, 3] still propose grammars and languages for SLA modeling but they focus on the IoT application scenario. In particular, Alqahtani et al. [43] design an SLA grammar that considers workflow activities and the multi-layered nature of IoT applications. They developed a tool for SLA specification and composition that can be used as a template to generate SLAs in a machine-readable format and to provide a fine-grained level of user requirement specifications. Moreover, a rule-based recommendation system called IoT-CANE is intended to automatically suggest configuration knowledge artifacts to multiple layers, required for users during the IoT resource configuration management processes. To evaluate user satisfaction with IoT-CANE, the authors conduct a user study with domain experts. In the extension presented in [44] the authors propose an enhanced version of the same grammar that achieves 91.70% of generality and 93.43% of expressiveness and it has been evaluated through a GQM

²<http://www.w3.org/TR/owl-ref/>

Table 4: Publications related to SLA modeling

Paper	Year	Modeling Type	Validation	Domain
García, et al. [38]	2017	Ontology	Custom tool	Cloud
Scoca, et al. [45]	2017	Language	IDEAS software	Web Service
Labidi et al. [40]	2018	Ontology	Cloud SLA Monitoring Ontology (CSLAMOnto)	Cloud
Kapassa et al. [47]	2018	Template	-	5g Network
Labidi et al. [39]	2018	Ontology	Cloud SLA Analyzing (CSL2A)	Cloud
Engel et al. [42]	2018	Language	ysla Engine	Cloud
Alqahtani et al. [43, 44]	2018, 2019	Grammar	Human experts	IoT
Uriarte et al. [26]	2019	Language	Custom tool	Cloud
Noureddine et al. [3]	2021	Language	DSL	IoT

approach. In the proposal of [3] ML-SLA-IoT, a framework for IoT SLA specification and monitoring is presented. The language specification part exploits the functionalities of the Domain-Specific Language (DSL) technique. A DSL is a programming domain-specific language designed to provide solutions to the problems raised in a particular field. ML-SLA-IoT describes QoS levels, provided services, and obligations. Moreover, compared to other SLA specification languages, it allows the specification of user preferences, reuse of microservices, and use of ML-SLA (multi-level metrics and QoS according to existing constraints and user preferences).

Differently from the above works, in [47] the authors try to map high-level requirements, expressed by users in SLAs, to low-level network parameters included in policies. Their platform, called 5GTANGO, includes an SLA Generator that creates both the SLA templates for the Service/Infrastructure provider and the final SLA itself.

In Table 4, we report a summarized view of the publications related to the modeling phase of the SLA life cycle, identifying the type of modeling (i.e., ontology, language, grammar or template), the method used to validate the approach, and the application domain.

Several approaches do not specifically design a modeling method but propose approaches supporting this phase of the SLA life cycle [48, 49]. In this sense, a further step has been conducted by Ganapathy and Joshi [48]. Here the authors develop a framework to automate the process of extracting knowledge embedded in Cloud SLAs and representing it in a semantically rich knowledge graph. In this case, the textual SLA in input is processed with the help of Semantic Web technologies and text mining techniques. Moreover, the extracted components are, then, stored through the usage of OWL and RDF graphs.

Finally, another research still related to the proposals described in this section but not directly focusing on SLA modeling has been carried out in [49]. In particular, SLA elements are conceptualized to support their analysis and comparison through an ontological representation. The proposed ontology focuses on SLA indicators and technical parameters and is built by exploiting the OWL2-RL language.

5.2 SLA Negotiation

In this section, we review research works proposing approaches for SLA negotiation. SLAs are defined before service usage and are based on a negotiation stage between provider and consumer. This phase can happen autonomously provider-side within any number of constraints, or can be performed interactively, thus supporting more dynamic service environments. In any case, it aims at maximizing revenues while minimizing the service cost to both parties, realigning the delivered service with the current business strategies. In most of the existing negotiation protocols, SLA templates or profiles are offered by the service provider, either represented by humans or by an SLA manager service, to initiate the negotiation. Negotiation between customers and providers is usually achieved through a negotiation protocol.

Two key approaches can be used during this phase of the SLA life cycle, namely *bargaining-based* negotiation (or *brokering*) and *offer-based* negotiation [50]. In the first case, SLA managers, acting as brokers, leverage the service offering or catalog model for customers who choose services based on their preferences. In this type of negotiation, both parties can make offers and counteroffers until an agreement is reached. In the latter case, instead, the SLA manager helps the provider to allocate the resources as needed, providing some offers with various SLO levels to achieve the expected requirements.

A further categorization for this phase is based on the number of parties involved. Negotiation can be classified as *bilateral* (or one-to-one) and *multilateral* (one-to-many). Bilateral negotiation is performed directly and it is one of the most widely used negotiation styles. Multilateral negotiation, instead, is used in Cloud environments, where providers compete with one another to attract customers. Usually, it takes place when a customer sends service requirements to a negotiation broker to find the most suitable service from providers at a low cost.

A subsequent process, especially useful in Cloud environments and known as renegotiation, is also available to alter the terms of an existing agreement. In the SLA life cycle, it is placed after the SLA Monitoring stage and allows customers and providers to initiate changes in an established agreement before service/resource reconfiguration.

Renegotiation can be proactive or reactive. In the first case renegotiation can happen in two ways, namely:

- the customer begins the renegotiation to support the changing requirements before service termination;
- the provider initiates the renegotiation to prevent any violation of the agreed-on service level due to some unexpected environmental change.

In the reactive case, instead, when any SLA violation is detected, renegotiation takes place instead of the termination of the service.

In the following, we review several contributions related to SLA negotiation and renegotiation phases.

The papers described in [51, 52, 45, 53, 54, 55] propose negotiation mechanisms that use distributed service brokers to dynamically negotiate with service providers on behalf of service consumers. The model described in [51], called IoT-Negotiate, relies on a hierarchical topology to address the communication challenges in an IoT environment, performs location-based data distribution and replication to enable efficient message forwarding, and conducts distributed SLA negotiation with candidate service providers. The proposal of [52], instead, relies on a Multi-Criteria Decision Making (MCDM) method to maximize a utility function so that the customer can choose services with the required QoS performances. Also, a negotiation model for the SLA and a context-based SLA contract ontology in IP Multimedia Subsystem (IMS) is designed. The work in [45] proposes a methodology for SLA autonomous negotiation. The presented framework checks the consistency of the specification, analyzes the compatibility between offers and requests and finds the best possible agreement (if any) by leveraging utility functions and the level of flexibility offered by providers and consumers.

Similarly, more recent works [53, 56, 55, 57, 54, 58] illustrate negotiation frameworks in Cloud relying on intelligent agents as third parties. In particular, [53] describes an Intelligent Automated Negotiation Agent (IANA) designed to meet the dynamic needs of compound services in a Cloud environment to negotiate SLA agreements. In [54], an automated dynamic SLA negotiation framework, called ADSLANF, is proposed. It uses a dynamic SLA concept to negotiate service terms and conditions through negotiation mechanisms based on game theory and a third-party broker agent. An Intelligent Recommender and Negotiation Agent Model (IRNAM) is illustrated in [55]. Firstly, it aims to recommend and select matching Cloud server providers and, then, it finalizes the SLA to achieve consensus based on the satisfaction level for all the parties. Because the recommendation phase deals with the choice of a particular provider, the negotiation style is bilateral.

The authors of [59] adopt a different perspective allowing users in a multi-cloud environment to express their requirements in Cloud plan selection. This facility, which is a particular kind of service negotiation, is also known as “services selection” and it is carried out using SLA. After identifying user requirements, they illustrate possible approaches to rank Cloud plans based on users’ preferences according to loud exposed SLA. This approach can be used in brokerage services, to evaluate offers by different providers, as well as in single-provider scenarios, to evaluate the different plans (possibly resulting from customization) offered by a provider. Also, the approaches presented in [60, 61] select the optimal combination of services, from multiple Cloud providers, that best satisfy the customer requirements, relying on exposed SLA. In particular, the approach in [61] leverages a fuzzy-based brokering service for Cloud plan selection that allows users to specify their requirements using natural language expressions. Fuzzy logic and fuzzy inference systems are adopted to assess the compliance of Cloud services quantitatively expressed through SLA and hence help users in the Cloud service selection process.

Several contributions rely on *offer-based* negotiation [26, 57, 58, 62]. The authors of [26] introduce SLAC, an SLA definition language for Cloud environments. SLAC supports the SLA life cycle and the definition of templates for the negotiation phase to discover the compatibility of offers and requests. In this paper, the authors do not deep dive into negotiation aspects, but they consider that all involved parties have a Negotiator component that proposes SLAs and evaluates requests for both negotiation, renegotiation, or modifications in the SLA. An Automated Negotiation System (ANS) for SLA negotiation of composite Cloud services is proposed in [57]. It deals with the design and development of a novel negotiation strategy that considers three factors for generating proposals, namely: time, negotiators’ preferences, and a negotiation method called opponent’s behavior. This method attempts to generate a proposal that provides

Table 5: Publications related to SLA negotiation

Paper	Year	Service Type	Negotiation style	Renegotiation type	Domain
Scoca et al. [45]	2017	Brokering	Multilateral	-	Cloud
Di Vimercati et al. [59]	2017	Brokering	Multilateral	-	Cloud
Paputungan et al. [65]	2018	-	-	Proactive	Cloud
Li et al. [58]	2018	Offering	Multilateral	-	Cloud
Li et al. [51]	2019	Brokering	Multilateral	-	IoT
Uriarte et al. [26]	2019	Offering	Bilateral	Proactive	Cloud
Li et al. [63]	2019	Brokering	Bilateral	-	Cloud
Di Vimercati et al. [61], Shojaiemehr et al. [57]	2019	Brokering	Multilateral	-	Cloud
Labidi et al. [66]	2020	Offering	Multilateral	Reactive	Cloud
Haddar et al. [52]	2020	Brokering	Multilateral	-	IMS
Li et al. [62]	2021	Offering	Bilateral	-	IoT
Rajavel et al. [54]	2021	Brokering	Multilateral	-	Cloud
Kumar et al. [53], Ibrahim et al. [56]	2023	Brokering	Multilateral	-	Cloud
Kumar et al. [55]	2023	Brokering	Bilateral	-	Cloud

higher utility for the customers relying on their proposals. The paper [58] takes a different direction by designing an Agent-based Fuzzy Constraint-directed Negotiation (AFCN) model for SLA negotiation that supports an iterative many-to-many infrastructure that does not require a broker to coordinate the negotiation process. To consider the behavior of different agents, this model can also adopt different negotiation strategies, such as competitive, win-win, and collaborative strategies in different Cloud computing environments. Similarly, in [62, 63], the authors address the problem of SLA negotiation candidates selection in IoT through a trust model designed to help Cloud entities make service decisions. In particular, in [62], they design this trust model to identify trusted service providers before attempting to negotiate an SLA. The solution leverages both Rough Set theory to predict the negotiation success rate, and Bayesian inference to deduce the possibility of SLA violations according to the monitored data. By contrast, the work presented in [63] equips brokers with a learning module enabling them to capture implicit service demands and find user preferences.

Differently from the previous proposals, the authors of [64] focus on a particular problem related to SLA negotiation. Specifically, they design an approach to allow service providers to check, at design time, whether a composed Web service with temporal parameters will always satisfy the temporal constraints specified in an SLA.

The SLA renegotiation phase is considered in [65, 66]. In particular, the paper presented in [65] introduces an extension of the SLA management life cycle for enabling SLA renegotiation during service delivery. In particular, a real-time and proactive SLA renegotiation model for dynamic Cloud-based environments is proposed. To achieve real-time decisions, a multi-offer generation approach is used and a mechanism to detect and predict service violations is used to ensure proactive renegotiation. The strategy proposed in [66], instead, models both negotiation and renegotiation phases. The style of negotiation considered is multilateral, indeed, in this approach there are several participants, both vendors offering their products and buyers submitting bids. Moreover, it relies on an ontological representation to semantically represent the client’s requirements and the provider’s offers. The renegotiation stage is automatically triggered during runtime once an unexpected variation in the Cloud service context is detected.

In Table 5, we report a summarized view of the publications related to the negotiation phase of the SLA life cycle, identifying the type of service (i.e., brokering or offering), the style of negotiation related to the number of parties involved (i.e., bilateral or multilateral), the type of renegotiation if considered in the paper (i.e., proactive or reactive), and the application domain.

An alternative approach to renegotiation is presented in [67] and it is called Multi-Level SLA (ML-SLA). ML-SLA supports the dynamic change of service levels with price adjustments to overcome the limited flexibility issues coming from the traditional static SLA approaches. Compared to traditional SLA approaches with renegotiation, in the Multi-Level SLA approach services do not have to be terminated or interrupted and level switches require less time and effort.

5.3 SLA Monitoring and Violation

The monitoring process in the SLA life cycle aims to capture the performance of physical and virtual servers continuously, the network, the shared resources, and the applications running on top of them [50].

Monitoring can be used to detect whether an SLA has been violated. Predicting possible SLA violations can be useful in proactively maintaining the SLAs. By monitoring resource utilization, the service provider can study past disappointments and avoid them in the first occurrence.

When the service lifetime is expiring or when any unacceptable violation has occurred, the contract of service termination would be initiated by either the service provider or the customer. In the latter case, the service provider incurs a penalty. Specifically, SLA violations can be due to one of the following reasons[68]:

- Defective performance, i.e., the monitored parameters have lower levels.
- Late performance, the service is provided at the appropriate level but with unjustified delays.
- The service is not provided at all.

Any type of breakdown has consequences regarding customer satisfaction and may result in a violation of an SLA [69].

In the following, we describe recent approaches defining solutions for SLA monitoring, violation, or prediction of violation.

In particular, the proposals of [70, 71, 72] focus on SLA monitoring. The authors of [70] describe a threshold method for preserving SLA parameters for Trusted IaaS Cloud. They identify particular SLA metrics to monitor to assess the status of the service provisioning. If they recognize that the value is less than a threshold value, then precautionary actions are taken to avoid breaching the SLA. In [71], the authors propose SLA-Monitoring as a Service (SLA-MaaS), a framework for monitoring providers' services by adopting third-party monitoring services with SLA and penalties management. The violation part is handled via a three-layer penalties approach, i.e., if a violation occurs, the system starts from a warning and applies lower penalties, instead of directly terminating the SLA. In [72], the authors describe a mechanism for SLA monitoring using Reinforcement Learning (RL) and a Long short-term memory (LSTM) network for the prediction of Cloud resources.

The authors of [73, 74, 75] propose approaches dealing with SLA violations. In particular, Singh and Goraya [73] propose an automatic multiagent framework that ensures the minimization of the SLA violation rate in workload execution. A negotiation agent selects the best service that can execute the current workload without SLA violation and with minimum consumption of energy. A monitoring agent has to continuously monitor for SLA violations, whereas another agent keeps track of workload executions to provide better forecasts of future executions. Similarly to this approach, [74] presents a method that identifies the physical hosts' workloads before the overflow energy consumption in a Cloud environment, while also reducing SLA violation. This approach predicts the load of physical hosts through both an energy-conscious model and a granular neural network. In [75], a generic SLA ontology is created to develop an expert system called SLAVIDES using it. This framework aims to detect SLA violations, check constraints, and make inferences. Since the ontology is designed as generic, it is intended to be used in many different knowledge domains.

Differently, the proposal of Uriarte et al. [26] defines SLAC, as an SLA definition language for Clouds to support the whole SLA life cycle, including the monitoring phase. The penalty and billing enforcement module is invoked only after termination, hence, the violation phase is not included in the described module. To perform monitoring, SLAC uses a component called SLA Inspector parses the data received from the Monitor module and generates a set of constraints. The satisfiability of these constraints is, then, checked against the SLA constraints using the Z3 solver [76], a Satisfiability Modulo Theories (SMT) solver from Microsoft Research.

Other more recent studies [77, 78, 79] apply Machine Learning (ML) models to a large IT service dataset to predict whether an incident involves a violation of SLA conditions. In particular, [77] makes a comparison of ML models and applies them to a large IT services incident dataset. The authors found that logistic regression and neural network models have the best performance in terms of misclassification rates and average squared error. This investigation can be useful for proactive incident management. The work in [79] explores four diverse ML-based predictors (i.e., logistics regression, artificial neural network, random forest, and extreme gradient boosting) to detect and predict SLA violations. Instead, [78] exploits an ML technique based on the Learning Classifier System (LCS) to detect violations.

A consistent group of proposals adopts Blockchain technology for its potential to support monitoring or violation detection approaches without the use of trusted third parties, guaranteeing the integrity of the client's logs[80, 81, 3, 82, 83, 84, 85, 86, 87]. In particular, the authors of [81] leverage a public Blockchain and a log-based algorithm to detect SLA violations in the Cloud. SLA parameters are monitored by the service provider using the agreed SLA template. The proposals of [3, 87, 88] relies on Blockchain and smart contracts to monitor the SLA terms without the

intervention of a third party. The authors of [88] propose to verify the SLA using an integrity-checking method based on a distributed ledger. The framework called ML-SLA-IoT [3] automatically generates smart contracts from the SLOs, these smart contracts are responsible for tracking the Service Level Objective parameters, detecting violations, and notifying the service provider. The proposal of [82] consists of a decentralized approach for enforcing the consequences of SLA violations. It relies on smart contracts to address incidents and automate decision-making on the compliance level of providers. The authors of [83] include in their framework a two-level Blockchain architecture. At the first level, the smart SLA is transformed into a smart contract, based on SLAC[26]. At the second level, a permissioned Blockchain is in charge of generating objective measurements for the smart SLA/contract assessment. Instead, the work of [80] focuses on fog computing, while the proposal described in [84] designs SLAM, a framework for continuous SLA monitoring in a multi-cloud ecosystem. Similar to the above papers, it is based on Blockchain and leverages smart contracts to detect SLA violations, but it determines the violations' root causes through a hierarchical system structure. Analogously, the proposal of [86] relies on a Blockchain network for SLA violation detection. Moreover, it provides an interface for both the Cloud service provider and clients to access and store the violation logs in an immutable system. The framework illustrated in [85] is composed of an SLA monitoring module developed using the auto-scaling feature of OpenStack Hadoop Service, a violation and logging module implemented through Blockchain. Moreover, the framework includes an algorithm to compensate the users based on the number of violations and the type of subscription. The proposal of [89] relies on several witnesses to perform SLA monitoring and detect violations. These actors must behave honestly to gain the maximum profit for themselves, which can be proved by a game theory strategy. Compensation in case of violation is automatically transferred to the customer leveraging a Blockchain smart contract.

In Table 6, we report a summarized view of the publications related to both the monitoring and violation phases, because, as seen before, these two stages of the SLA life cycle are closely linked together. This table shows if the cited paper presents an approach for monitoring, violation, or violation prediction, the technique it applies, and the application domain.

Finally, we consider the compensation process strictly related to the SLA violation phase. Indeed, in the last phase of the SLA management life cycle, in case any violation is encountered during the SLA monitoring phase, the compensation process occurs and penalties are enforced. In this direction, the paper presented in [90] provides a framework for the translation of QoS-related SLAs in Blockchain-based smart contracts as done in [83, 26]. Moreover, it automates SLA compensation and service fee payments relying on Blockchain.

6 Security and Privacy SLA

In the current Cloud and IoT scenarios, security assurance and transparency continues to be a significant issue given (i) the growing number of both devices and Cloud servers offering diverse services, (ii) new and heterogeneous architectures, and (iii) the vulnerability to information disclosure and service unavailability of such environments.

Regular SLAs usually concern quantitative and measurable indicators of performance-related Service Level Objectives (SLOs), mainly concerning the availability of service, the response time, and the Quality of Service (QoS). Hence they did not provide coverage of security metrics by definition.

Although security has been considered for decades as a possible attribute in SLAs [5], the problem of establishing measurable and shared metrics in this context makes it difficult for researchers and practitioners to design solutions to include security guarantees in their SLAs, explicitly. Hence, finding approaches for managing security in SLA for all the phases of its life cycle (including negotiation, enforcement, and monitoring phases) is still an open challenge and work needs to be done in this direction [6].

Only recently, Security SLAs (SecSLAs) have been introduced to pave the way for the inclusion of security aspects in service provisioning. Like the traditional SLA, the life cycle of SecSLAs comprises several stages each defining a specific role held by either the customer or the service provider:

- **Definition.** This phase includes the specification of the security parameters and metrics possessed by a SecSLA.
- **Negotiation.** In this phase, the security requirements are planned by the different actors of the systems. If present, a Cloud broker can initiate its evaluation process.
- **Deployment.** In this phase, the needed security services are deployed through the implementation of security mechanisms.
- **Monitoring and Reporting.** After its execution, the SecSLA is continuously monitored. Moreover, during this last phase, multiple actions may take place, namely, (i) the reporting of security and performance levels,

Table 6: Publications related to SLA Monitoring and Violation

Paper	Year	Monitoring	Violation	Prediction	Domain
Karamanlioglu and Alpaslan[75]	2018	✓(expert system)	-	-	-
Zhou et al. [89]	2018	✓(witnesses)	✓(witnesses)	-	Cloud
Uriarte et al. [26]	2019	✓(Z3 solver)	-	-	Cloud
Wonjiga et al. [88]	2019	✓(Blockchain)	-	-	Cloud
Prasad et al. [70]	2020	✓(threshold)	-	-	IaaS
Prasad et al. [72]	2020	✓(RL)	-	✓(LSTM)	Cloud IoT-based
Alzubaidi et al. [82]	2020	-	✓(Blockchain)	-	IoT
Ranchal and Choudhury[84]	2020	-	✓(Blockchain)	-	Multi-Cloud
De Brito et al. [87]	2020	✓(Blockchain)	-	-	Cloud
Subeh and Al-Ajeli [78]	2021	-	-	✓(LCS)	Business processes
Noureddine et al. [3], Uriarte et al. [83]	2021	✓(Blockchain)	-	-	IoT
Pandey et al. [85]	2021	✓(log analysis)	✓(Blockchain)	-	Cloud
Abhishek et al. [86]	2021	-	✓(Blockchain)	-	Multi-Cloud
Zeng et al. [79]	2021	-	✓(ML)	✓(ML)	Web services
Battula et al. [80]	2022	-	✓(Blockchain)	-	Fog Computing
Badshah et al. [71]	2023	✓(SLA-MaaS)	✓(three-layer penalties)	-	Cloud
Neeraj et al. [81]	2023	✓(log analysis)	✓(Blockchain)	-	Cloud
Singh and Goraya [73]	2023	✓(agent)	✓(agent)	✓(agent)	Cloud
Swain and Garza [77]	2023	-	-	✓(ML)	IT services

(ii) the prediction of contract violations, (iii) the management of corrective actions, and (iv) the implementation of incident response and remediation plans.

To enforce and monitor security in Cloud and IoT environments, a report by the European Union Agency for Network and Information Security (ENISA) recommended the adoption of Security Service Level Agreements (Security SLA). According to this report, a Security SLA (SecSLA) is defined as a contract between service providers and service customers stating the level of granted security between the parties[91, 92]. Also, several security metrics have been proposed in the context of European projects such as A4Cloud³, SPECS [93], and MUSA⁴ recently investigating the adoption of SLAs and Security SLAs in the Cloud by proposing models and frameworks for SLA definition and life cycle management. The SPECS project [93] is an example of such an effort. Its main purpose is to design a framework that offers Security-as-a-Service in a Cloud-based environment specifying the security parameters directly in the SLA, thus providing a way to manage its life cycle. A Security Metric Catalogue including 35 metrics is integrated into the machine-readable format proposed by the SPECS project for Security SLAs [94]. These metrics are compliant with the directions from ISO about the structure and format of metrics.

According to Chan et al., [95], there are several security properties or dimensions (i.e. availability, data confidentiality, data integrity, access control, authentication, non-repudiation, communication security, and privacy) from which specific security metrics can be computed and that can be potentially used as Security SLA attributes [22]. In particular:

³<https://a4cloud.eu/>

⁴<https://musa-h2020.eu/>

- Availability is a property including response and resolution times and is thought to guarantee the lack of denial of service (DOS attack) to the network and the services. The SLA parameter used to measure this metric is the percentage of downtime due to security incidents.
- Data confidentiality is intended to preserve sensitive data from unauthorized access or disclosure.
- Data integrity ensures the correctness of data against unauthorized modification or tampering attacks. The percentage of such attacks can provide a metric to measure this property.
- Access control guarantees that only authorized personnel or devices are allowed to access network elements, services, and applications.
- Authentication is a property applied to identify the communication entities against spoofing.
- Non-repudiation property involves the ability to give proof-of-origin to data or the cause of an event or an action. A possible metric for this property can be the percentage of the use of digital signatures.
- Communication security ensures that information flows only between authorized endpoints and can be measured through the percentage of hijacked time sessions.
- Privacy deals with the protection of information and identity of the involved actors.

In the last decade, a further specification of SecSLA has been defined in the context of the Cloud. It is known as the Privacy Level Agreement (PLA, hereafter) and it has been first defined by the Privacy Level Agreement Working Group of the Cloud Security Alliance (CSA) [96]. PLAs are similar to SecSLAs, but they deal only with concepts related to data protection practices [97, 98].

In the following, we start by describing the current research proposing approaches related to SecSLAs [99, 100, 101, 102, 103]. In [99], the authors propose a broker-based framework for SecSLA management in the Cloud. They design service selection based on security satisfaction and, to minimize the number of security breaches and incidents, they introduce a SecSLA monitoring model, a violation prediction, and a remediation process. Moreover, in this work, a set of measurable security metrics is developed. Another proposal [100] suggests including the security monitoring terms in IaaS Cloud SLAs. Moreover, it implements the monitoring phase of the SLA life cycle by evaluating production traffic in the case of anomaly-based Network IDSs (NIDSs). A continuously observed KPI represented as an SLO, is used in an SLA to verify the SLA itself and describe the performance of an NIDS. The authors of [101] propose a Security-by-Design methodology for the development of secure Cloud applications. This framework relies on SecSLA to specify the application security capabilities and quantifying the provided level of security. The adopted Security SLA model has been introduced in the SPECS project [93]. It is based on the WS-Agreement's XML schema standard, which has been extended to include Cloud provider-specific information and security-related guarantees. It aims at implementing a data model to collect security-related information (i.e., assets, threats, vulnerabilities) and a graph-based model to represent distributed Cloud applications. Thanks to these, the proposed automated methodology has been developed to support a tool for (i) security requirement identification performed by means of a risk analysis process, (ii) components (COTS) security assessments and (iii) Cloud application security assessment. The work of [102] presents a solution for security SLA creation for health service in multi-Cloud-based IoT including the specification of both security and privacy levels. It presents a methodology to quantitatively calculate security and privacy SLAs of IoT applications on top of standard controls. This is obtained by mapping the application components to the security control implementation and, then, to the security metrics. Nugraha and Martin [103] define Trustworthy Service Level Agreements (TSLA) as a mechanism for incorporating privacy parameters (especially confidentiality) into SLAs to preserve the confidentiality of government data against unauthorized access or disclosure. In the paper, they describe five discrete levels of security precautions applied to the formulation of security-related SLA.

A group of works specifically focuses on Privacy SLA (PLA, hereafter)[98, 104], which are specifications of SecSLA related only to privacy metrics. The study of [98] proposes the exploitation of PLAs in the context of Public Administration's (PA's) Information Systems with several objectives: (i) define citizens' privacy needs, (ii) provide feedback on data sharing, and (iii) enable PA departments to analyze privacy threats and vulnerabilities and compliance with laws and regulations. Instead, [104] presents a privacy-based SLA violation detection model for Cloud computing based on Markov decision process theory. This model can recognize and handle Cloud providers' actions based on users' requirements. Additionally, the model could evaluate the credibility of Cloud providers, and user privacy violations.

In Table 7 we report a summarized view of the publications related to the Security and Privacy Service Level Agreement. In particular, this table illustrates if a cited paper is based on a Security (SecSLA) or Privacy Level Agreement (PLA), which phase of the security life cycle is considered, and the paper's application domain.

Table 7: Publications related to Security and Privacy SLA

Paper	Year	SecSLA	PLA	Life cycle phase	Domain
Nugraha and Martin [103]	2017	✓	✓	Definition	Government Cloud
Diamantopoulou [98]	2017	-	✓	Definition, Monitoring and Reporting	PA
Zhou [104]	2017	-	✓	Monitoring and Reporting	Cloud
Halabi and Bellaiche [99]	2018	✓	-	Negotiation, Monitoring and Reporting	Cloud
Teshome et al. [100]	2018	✓	-	Monitoring and Reporting	IaaS Cloud
Casola et al. [101]	2020	✓	-	Definition, Negotiation, Monitoring and Reporting	Cloud
Rios et al. [102]	2022	✓	✓	Definition, Monitoring and Reporting	Multi-Cloud-based IoT

7 Open Issues and Future Directions

After performing our investigation, we have identified various challenges and open issues that can be explored to drive future research in the area. They mainly deal with SLA management, specifically regarding automation, standardization, integration, security and privacy, scalability, dynamic changes, and legal regulations [3].

- **Automation of SLA life cycle.** If carried out manually, the steps of the SLA management life cycle, comprising SLA creation, negotiation, monitoring, and violation, may result in expenses and errors. Guaranteeing that automated systems can interpret and respond appropriately to complex service metrics and contractual obligations is an ongoing challenge. Indeed, researchers and practitioners are endeavoring to develop automated software tools for the management of SLA documents [38].
- **Complexity and standardization.** Existing SLA languages focus on finding common formats or schemas, but often SLAs are technical documents related to terminology and concepts understandable by a specific class of specialists. Therefore, the complexity of services and the lack of standardized SLA frameworks across industries can contrast effective management. This trend is still open and the aim is to build solutions so that services can be described using mutually understandable terms and concepts [38].
- **SLA integration compatibility.** Especially for multi-cloud or IoT applications, where applications are distributed in diverse infrastructures and deployed in smart devices, SLAs are challenging to agree on due to the different standards adopted by providers, which are often proprietary and unable to interoperate. Ensuring consistency and compatibility across these platforms poses a significant challenge [20, 3]. Furthermore, for the IoT paradigm, issues of interdependence between devices may exist as the service provided by one of them could depend on the service provided by the others [15, 43].
- **Security and Privacy.** Incorporating security measures into SLAs and handling privacy concerns related to sensitive data pose ongoing challenges, yet too little research has been conducted about this topic (see Section 8 for numeric about this concept). This results in a lack of trust among parties about the security capabilities offered by providers. Measuring security capabilities is difficult and, consequently, assessing whether a service provides the same level of security precaution for all customers could be not doable[22]. Moreover, even if guaranteeing compliance with evolving data protection regulations is crucial, existing certification schemes are still at an early stage for service provisioning context [103]. Therefore, research for security metrics development for SLAs in the current Cloud and IoT environments have proven to be an important topic to be investigated and the establishment of universally accepted key performance indicators (KPIs) in this context should be addressed in the future.
- **Dynamic and real-time SLA management.** Adapting SLAs to the dynamic nature of current Cloud and IoT paradigms, thus guaranteeing real-time monitoring and adjustments, is still a goal. Systems need to respond promptly to modifications of service conditions and new dynamic negotiation algorithms should be designed [90]. This is a challenge, especially for Industry 5.0 scenarios, where SLA can be used to trace scalability issues [105].

Table 8: Amount of papers analyzed per topic

Topic	Amount of papers
SLA Modeling	11
SLA Negotiation	18
SLA Monitoring and Violation	18
Security and Privacy SLA	9

- **Legal and Contractual Challenges.** Legal ambiguities, particularly in international or multi-party agreements, are an open issue to be solved ensuring that SLAs are legally enforceable and aligning them with local regulations [106].

8 Summary and Conclusion

An SLA is a formal document in which a provider defines its level of quality of service assurance through the parameters of the non-functional requirements, usually related to availability and performance. Recently, especially in the context of Cloud computing and the Internet of Things, researchers have investigated new approaches involving the integration of security metrics in SLA to guarantee security assurance and transparency.

To highlight a contribution in this setting, in this survey paper, we provided a detailed review of the most meaningful research papers focusing on SLA management and Security SLA. Following our proposed selection criteria, we comprehensively examined the most relevant and recent works, including those dealing with the definitions and principles of an SLA, language specifications, and the main steps of its life cycle. Furthermore, this survey paper also addresses the topics of security and privacy SLA management. Finally, we discussed the main challenges and future research directions in this context. In summary, we analyzed 56 research articles published in renowned international conferences, journals, symposiums, and workshops with a focus on SLA and SecSLA management and related areas. Table 8 and Figure 5 illustrate a quantitative overview of the reviewed literature divided into topics, whereas Figure 4 visualizes the total analyzed number of articles published per year.

As visible in both the table and two figures above, we can affirm that the analyzed papers are distributed according to our classification criteria, as follows: SLA modeling (20%), SLA negotiation(32%), SLA monitoring and violation (32%), security and privacy SLA (16%). The limited attention given to the latter phase, whose percentage has decreased to 6% in the last three years, may be attributed to the exploratory nature of most research efforts.

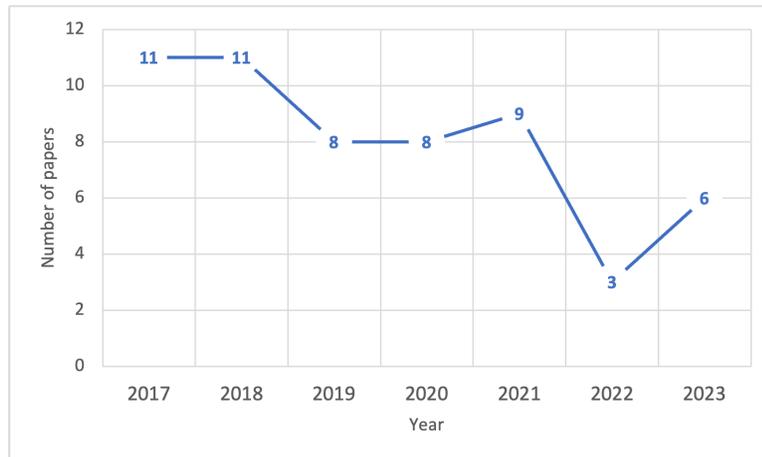


Figure 4: Literature timeline

We plan to continue our study by diving into particular aspects only mentioned in this survey. For instance, an interesting direction can be the review of the papers exploiting existing SLA industrial platforms to give the reader a more extensive spectrum of various issues about them. Moreover, an exhaustive description of all the application domains in the context of IoT can be also a challenging task.

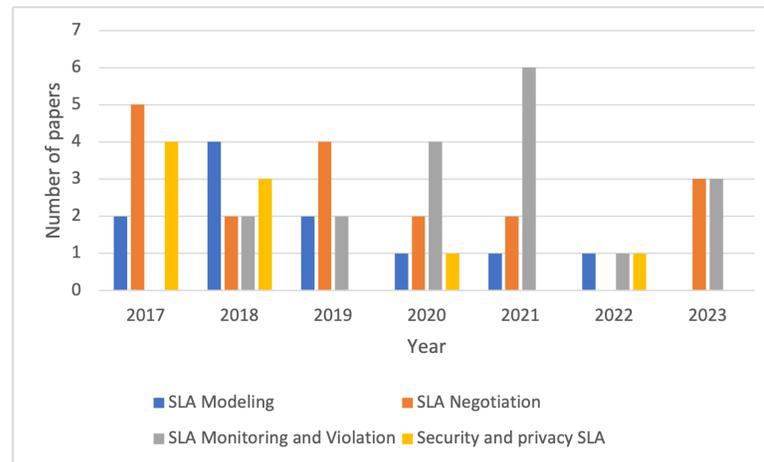


Figure 5: Literature timeline per topic

We hope that this survey can assist both academic researchers and industrial practitioners in apprehending the key features of this domain, highlighting the most significant advancements and perspectives, and encouraging them to undertake this direction in future research advancements.

Acknowledgments

This work was supported in part by the project SERICS (PE00000014) under the NRRP MUR program funded by the EU-NGEU, and by the PRIN Project “HOMEY: a Human-centric IoE-based Framework for Supporting the Transition Towards Industry 5.0” (code 2022NX7WKE) funded by the European Union - Next Generation EU.

References

- [1] Dimosthenis Kyriazis. Cloud computing service level agreements—exploitation of research results. *European Commission Directorate General Communications Networks Content and Technology Unit, Tech. Rep*, 5:29, 2013.
- [2] Svetlana Girs, Séverine Sentilles, Sara Abbaspour Asadollah, Mohammad Ashjaei, and Saad Mubeen. A systematic literature study on definition and modeling of service-level agreements for cloud services in iot. *IEEE Access*, 8:134498–134513, 2020.
- [3] Staifi Nouredine and Belguidoum Meriem. Ml-sla-iot: An sla specification and monitoring framework for iot applications. In *2021 International Conference on Information Systems and Advanced Technologies (ICISAT)*, pages 1–12, online, 2021. IEEE.
- [4] Aparna Bhonde and Satish Devane. Impact of cloud attacks on service level agreement. In *2021 International Conference on Communication information and Computing Technology (ICCICT)*, pages 1–6, Mumbai, India, 2021. IEEE.
- [5] Ronda R Henning. Security service level agreements: quantifiable security for the enterprise? In *Proceedings of the 1999 workshop on New security paradigms*, pages 54–60, Ontario, Canada, 1999. ACM.
- [6] Valentina Casola, Alessandra De Benedictis, and Massimiliano Rak. On the adoption of security slas in the cloud. *Accountability and Security in the Cloud: First Summer School, Cloud Accountability Project, A4Cloud, Malaga, Spain, June 2-6, 2014, Revised Selected Papers and Lectures 1*, 8937:45–62, 2015.
- [7] Kai Petersen, Sairam Vakkalanka, and Ludwik Kuzniarz. Guidelines for conducting systematic mapping studies in software engineering: An update. *Information and software technology*, 64:1–18, 2015.
- [8] IEEE.org. Ieee xplore. <https://ieeexplore.ieee.org>, 2024.
- [9] Elsevier. Scopus. <https://www.scopus.com>, 2023.
- [10] Google. Google scholar. <https://scholar.google.com>, 2024.
- [11] Association for Computing Machinery (ACM). Ac digital library. <https://dl.acm.org>, 2024.

- [12] Scimago Lab. Scimago. <https://www.scimagojr.com/>, 2024.
- [13] Computing Research & Education. CORE Conference Portal. <https://portal.core.edu.au/conf-ranks>, 2023.
- [14] Saad Mubeen, Sara Abbaspour Asadollah, Alessandro Vittorio Papadopoulos, Mohammad Ashjaei, Hongyu Pei-Breivold, and Moris Behnam. Management of service level agreements for cloud services in iot: A systematic mapping study. *IEEE access*, 6:30184–30207, 2017.
- [15] Alessandro Vittorio Papadopoulos, Sara Abbaspour Asadollah, Mohammad Ashjaei, Saad Mubeen, Hongyu Pei-Breivold, and Moris Behnam. Slas for industrial iot: Mind the gap. In *2017 5th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)*, pages 75–78, Prague, Czech Republic, 2017. IEEE.
- [16] Jinyuan He and Le Sun. A review on sla-related applications in cloud computing. In *2018 1st International Cognitive Cities Conference (IC3)*, pages 87–91, Okinawa, Japan, 2018. IEEE.
- [17] Vivek Kumar Prasad and Madhuri Bhavsar. Efficient resource monitoring and prediction techniques in an iaas level of cloud computing: Survey. In *Future Internet Technologies and Trends: First International Conference, ICFITT 2017, August 31-September 2, 2017, Proceedings 1*, pages 47–55, Surat, India, 2018. Springer.
- [18] Nawel Hamdi, Chiraz El Hog, Raoudha Ben Djemaa, and Layth Sliman. A survey on sla management using blockchain based smart contracts. In *International Conference on Intelligent Systems Design and Applications*, pages 1425–1433, Seattle, WA, United States, 2021. Springer.
- [19] Isaac Odun-Ayo, Olasupo Ajayi, and Nicholas Omoregbe. Cloud service level agreements—issues and development. In *2017 International Conference on Next Generation Computing and Information Systems (ICNGCIS)*, pages 1–6, Jammu, India, 2017. IEEE.
- [20] Isaac Odun-Ayo, Blessing Udemezue, and Abiodun Kilanko. Cloud service level agreements and resource management. *Adv. Sci. Technol. Eng. Syst.*, 4(2):228–236, 2019.
- [21] Yogesh Sharma, Deval Bhamare, Nishanth Sastry, Bahman Javadi, and Rajkumar Buyya. Sla management in intent-driven service management systems: A taxonomy and future directions. *ACM Computing Surveys*, 55(13):1–38, 2023.
- [22] Yudhistira Nugraha and Andrew Martin. Understanding trustworthy service level agreements: Open problems and existing solutions. In *International Workshop on Open Problems in Network Security (iNetSec)*, pages 54–70, Rome, Italy, 2017. Springer.
- [23] Carlos André Batista De Carvalho, Rossana Maria de Castro Andrade, Miguel Franklin de Castro, Emanuel Ferreira Coutinho, and Nazim Agoulmine. State of the art and challenges of security sla for cloud computing. *Computers & Electrical Engineering*, 59:141–152, 2017.
- [24] Edward Wustenhoff and Sun BluePrints. Service level management in the data center. *Sun BluePrints Online*, 1:2–13, 2002.
- [25] Li-jie Jin, Vijay Machiraju, and Akhil Sahai. Analysis on service level agreement of web services. *HP June*, 19:1–13, 2002.
- [26] Rafael Brundo Uriarte, Rocco De Nicola, Vincenzo Scoca, and Francesco Tiezzi. Defining and guaranteeing dynamic service levels in clouds. *Future Generation Computer Systems*, 99:27–40, 2019.
- [27] Alexander Keller and Heiko Ludwig. The wsla framework: Specifying and monitoring service level agreements for web services. *Journal of Network and Systems Management*, 11:57–81, 2003.
- [28] Adil Maarouf, Abderrahim Marzouk, and Abdelkrim Haqiq. A review of sla specification languages in the cloud computing. In *2015 10th International Conference on Intelligent Systems: Theories and Applications (SITA)*, pages 1–6, Rabat Morocco, 2015. IEEE.
- [29] Heiko Ludwig, Alexander Keller, Asit Dan, Richard P King, and Richard Franck. Web service level agreement (wsla) language specification. *Ibm corporation*, 1:815–824, 2003.
- [30] Alain Andrieux, Karl Czajkowski, Asit Dan, Kate Keahey, Heiko Ludwig, Toshiyuki Nakata, Jim Pruyne, John Rofrano, Steve Tuecke, and Ming Xu. Web services agreement specification (ws-agreement). In *Open grid forum*, volume 128(1), page 216, European Union, 2007. Citeseer, StandICT.eu.
- [31] Keven T Kearney, Francesco Torelli, and Constantinos Kotsokalis. Sla*: an abstract syntax for service level agreements. In *2010 11th IEEE/ACM International Conference on Grid Computing*, pages 217–224, Brussels, Belgium, 2010. IEEE, IEEE.
- [32] Yousri Kouki, Thomas Ledoux, et al. Csla: A language for improving cloud sla management. In *CLOSER*, pages 586–591, Porto, Portugal, 2012. Springer.

- [33] Yousri Kouki, Frederico Alvares De Oliveira, Simon Dupont, and Thomas Ledoux. A language support for cloud elasticity management. In *2014 14th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing*, pages 206–215, Chicago Illinois, 2014. IEEE.
- [34] Rafael Brundo Uriarte, Francesco Tiezzi, and Rocco De Nicola. Slac: A formal service-level-agreement language for cloud computing. In *2014 IEEE/ACM 7th International Conference on Utility and Cloud Computing*, pages 419–426, London, United Kingdom, 2014. IEEE.
- [35] Adrian Paschke. Rbsla a declarative rule-based service level agreement language based on ruleml. In *International Conference on Computational Intelligence for Modelling, Control and Automation and International Conference on Intelligent Agents, Web Technologies and Internet Commerce (CIMCA-IAWTIC'06)*, volume 2, pages 308–314, Vienna, Austria, 2005. IEEE.
- [36] Harold Boley, Said Tabet, and Gerd Wagner. Design rationale for ruleml: A markup language for semantic web rules. In *SWWS*, volume 1, pages 381–401, California, 2001. CEUR-WS.org.
- [37] Awatif Alqahtani, Ellis Solaiman, Rajkumar Buyya, and Rajiv Ranjan. End-to-end qos specification and monitoring in the internet of things. *IEEE Technical Committee on Cybernetics for Cyber-Physical Systems*, 1:9–13, 2016.
- [38] José María García, Pablo Fernández, Carlos Pedrinaci, Manuel Resinas, Jorge Cardoso, and Antonio Ruiz-Cortés. Modeling service level agreements with linked usdl agreement. *IEEE Transactions on Services Computing*, 10(1):52–65, 2017.
- [39] Taher Labidi, Achraf Mtibaa, and Faiez Gargouri. Cloud sla terms analysis based on ontology. *Procedia Computer Science*, 126:292–301, 2018.
- [40] Taher Labidi, Achraf Mtibaa, Walid Gaaloul, Samir Tata, and Faiez Gargouri. Cloud sla modeling and monitoring. In *2017 IEEE International Conference on Services Computing (SCC)*, pages 338–345, Honolulu, HI, USA, 2017. IEEE, IEEE.
- [41] Christian Bizer, Tom Heath, and Tim Berners-Lee. Linked data: The story so far. In *Semantic services, interoperability and web applications: emerging concepts*, pages 205–227. IGI global, Hershey, Pennsylvania, USA, 2011.
- [42] Robert Engel, Shashank Rajamoni, Bryant Chen, Heiko Ludwig, and Alexander Keller. ysla: reusable and configurable slas for large-scale sla management. In *2018 IEEE 4th international conference on collaboration and internet computing (CIC)*, pages 317–325, Philadelphia, PA, USA, 2018. IEEE.
- [43] Awatif Alqahtani, Yin hao Li, Pankesh Patel, Ellis Solaiman, and Rajiv Ranjan. End-to-end service level agreement specification for iot applications. In *2018 International Conference on High Performance Computing & Simulation (HPCS)*, pages 926–935, Orléans, France, 2018. IEEE.
- [44] Awatif Alqahtani, Ellis Solaiman, Pankesh Patel, Schahram Dustdar, and Rajiv Ranjan. Service level agreement specification for end-to-end iot application ecosystems. *Software: Practice and Experience*, 49(12):1689–1711, 2019.
- [45] Vincenzo Scoca, Rafael Brundo Uriarte, and Rocco De Nicola. Smart contract negotiation in cloud computing. In *2017 IEEE 10th international conference on cloud computing (CLOUD)*, pages 592–599, Honolulu, Hawaii, United States, 2017. IEEE.
- [46] Rafael Brundo Uriarte, Francesco Tiezzi, and Rocco De Nicola. Dynamic slas for clouds. In *Service-Oriented and Cloud Computing: 5th IFIP WG 2.14 European Conference, ESOC 2016, September 5-7, 2016, Proceedings 5*, pages 34–49, Vienna, Austria, 2016. Springer.
- [47] Evgenia Kapassa, Marios Touloupou, Argyro Mavrogiorgou, and Dimosthenis Kyriazis. 5g & slas: Automated proposition and management of agreements towards qos enforcement. In *2018 21st Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN)*, pages 1–5, Paris, France, 2018. IEEE.
- [48] Divya Natolana Ganapathy and Karuna Pande Joshi. A semantically rich framework to automate cloud service level agreements. *IEEE Transactions on Services Computing*, 16(1):53–64, 2022.
- [49] Antonella Longo, Domenico Potena, Emanuele Storti, Marco Zappatore, and Andrea De Matteis. Comparing slas for cloud services: A model for reasoning. In *New Trends in Databases and Information Systems: ADBIS 2018 Short Papers and Workshops, AI* QA, BIGPMED, CSACDB, M2U, September, 2-5, 2018, Proceedings 22*, pages 178–190, Budapest, Hungary, 2018. Springer.
- [50] Ahmad Fadzil M Hani, Irving Vitra Paputungan, and Mohd Fadzil Hassan. Renegotiation in service level agreement management for a cloud-based system. *ACM Computing Surveys (CSUR)*, 47(3):1–21, 2015.

- [51] Fan Li, Andrei Palade, and Siobhán Clarke. A model for distributed service level agreement negotiation in internet of things. In *Service-Oriented Computing: 17th International Conference, ICSOC 2019, October 28–31, 2019, Proceedings 17*, pages 71–85, Toulouse, France, 2019. Springer.
- [52] Imane Haddar, Brahim Raouyane, and Mostafa Bellafkih. Service broker-based architecture using multi-criteria decision making for service level agreement. *Computer and Information Science*, 13(1):1–20, 2020.
- [53] Rishi Kumar, Mohd Fadzil Hassan, and Muhamad Hariz M Adnan. Model of an intelligent and automated negotiation agent for the service level agreement negotiation process in cloud computing. *Journal of Advanced Research in Applied Sciences and Engineering Technology*, 32(2):189–202, 2023.
- [54] Rajkumar Rajavel, Sathish Kumar Ravichandran, Partheeban Nagappan, and Kanagachidambaresan Ramasubramanian Gobichettipalayam. Cloud service negotiation framework for real-time e-commerce application using game theory decision system. *Journal of Intelligent & Fuzzy Systems*, 41(5):5617–5628, 2021.
- [55] Rishi Kumar, Mohd Fadzil Hassan, Muhamad Hariz Muhammad Adnan, Saurabh Shukla, Sohail Safdar, Muhammad Aasim Qureshi, and Abdel-Haleem Abdel-Aty. A user-priorities-based strategy for three-phase intelligent recommendation and negotiating agents for cloud services. *IEEE Access*, 11:26932–26944, 2023.
- [56] Doaa Mohammed Ibrahim, Noha Ezzat Elatar, Weal Abdelkader Awad, and Ibrahim Mohamed Hanafy. Design and implementation an intelligent dynamic negotiation with third party for cloud computing. *Alfarama Journal of Basic & Applied Sciences*, 4(4):635–649, 2023.
- [57] Bahador Shojaiemehr, Amir Masoud Rahmani, and Nooruldeen Nasih Qader. A three-phase process for sla negotiation of composite cloud services. *Computer Standards & Interfaces*, 64:85–95, 2019.
- [58] Lin Li, Chee Shin Yeo, Chia-Yu Hsu, Liang-Chih Yu, and K Robert Lai. Agent-based fuzzy constraint-directed negotiation for service level agreements in cloud computing. *Cluster Computing*, 21:1349–1363, 2018.
- [59] Sabrina De Capitani Di Vimercati, Sara Foresti, Giovanni Livraga, Vincenzo Piuri, and Pierangela Samarati. Supporting user requirements and preferences in cloud plan selection. *IEEE Transactions on Services Computing*, 14(1):274–285, 2017.
- [60] Ahmed Taha, Salman Manzoor, and Neeraj Suri. Sla-based service selection for multi-cloud environments. In *2017 IEEE International Conference on Edge Computing (EDGE)*, pages 65–72, Honolulu, HI, USA, 2017. IEEE.
- [61] Sabrina De Capitani di Vimercati, Sara Foresti, Giovanni Livraga, Vincenzo Piuri, and Pierangela Samarati. A fuzzy-based brokering service for cloud plan selection. *IEEE Systems Journal*, 13(4):4101–4109, 2019.
- [62] Fan Li, Gary White, and Siobhán Clarke. A trust model for sla negotiation candidates selection in a dynamic iot environment. *IEEE Transactions on Services Computing*, 15(5):2565–2578, 2021.
- [63] Wenjuan Li, Jian Cao, Shiyu Qian, and Rajkumar Buyya. Tslam: a trust-enabled self-learning agent model for service matching in the cloud market. *ACM Transactions on Autonomous and Adaptive Systems (TAAS)*, 13(4):1–41, 2019.
- [64] Marco Franceschetti and Johann Eder. Checking temporal service level agreements for web service compositions with temporal parameters. In *2019 IEEE International Conference on Web Services (ICWS)*, pages 443–445, Milan, Italy, 2019. IEEE.
- [65] Irving Vitra Papatungan, Ahmad Fadzil Mohamad Hani, Mohd Fadzil Hassan, and Vijanth S Asirvadam. Real-time and proactive sla renegotiation for a cloud-based system. *IEEE Systems Journal*, 13(1):400–411, 2018.
- [66] Taher Labidi, Achraf Mtibaa, Walid Gaaloul, and Faiez Gargouri. Cloud sla negotiation and re-negotiation: An ontology-based context-aware approach. *Concurrency and Computation: Practice and Experience*, 32(15):e5315, 2020.
- [67] Philipp Grubitzsch, Iris Braun, Heiko Fichtl, Thomas Springer, Tenshi Hara, and Alexander Schill. MI-sla: multi-level service level agreements for highly flexible iot services. In *2017 IEEE International Congress on Internet of Things (ICIOT)*, pages 113–120, Honolulu, HI, USA, 2017. IEEE.
- [68] Omer Rana, Martijn Warnier, Thomas B Quillinan, and Frances Brazier. Monitoring and reputation mechanisms for service level agreements. In *Grid Economics and Business Models: 5th International Workshop, GECON 2008, August 26, 2008. Proceedings 5*, pages 125–139, Las Palmas de Gran Canaria, Spain, 2008. Springer.
- [69] Mohammed Alodib. Qos-aware approach to monitor violations of slas in the iot. *Journal of Innovation in Digital Ecosystems*, 3(2):197–207, 2016.
- [70] Vivek K Prasad and Madhuri Bhavsar. Preserving sla parameters for trusted iaas cloud: An intelligent monitoring approach. *Recent Patents on Engineering*, 14(4):530–540, 2020.

- [71] Afzal Badshah, Ateeqa Jalal, Umar Farooq, Ghani-Ur Rehman, Shahab S Band, and Celestine Iwendi. Service level agreement monitoring as a service: an independent monitoring service for service level agreements in clouds. *Big Data*, 11(5):339–354, 2023.
- [72] Vivek Kumar Prasad and Madhuri D Bhavsar. Monitoring and prediction of sla for iot based cloud. *Scalable Computing: Practice and Experience*, 21(3):349–358, 2020.
- [73] Jaspal Singh and Major Singh Goraya. An autonomous multi-agent framework using quality of service to prevent service level agreement violations in cloud environment. *International Journal of Advanced Computer Science and Applications*, 14(3):1–11, 2023.
- [74] Farnaz Mahan, Seyyed Meysam Rozekhani, and Witold Pedrycz. A novel resource productivity based on granular neural network in cloud computing. *Complexity*, 2021:1–15, 2021.
- [75] Alper Karamanlioglu and Ferda Nur Alpaslan. An ontology-based expert system to detect service level agreement violations. In *Business Modeling and Software Design: 8th International Symposium, BMSD 2018, July 2-4, 2018, Proceedings 8*, pages 362–371, Vienna, Austria, 2018. Springer.
- [76] Leonardo De Moura and Nikolaj Bjørner. Z3: An efficient smt solver. In *International Conference on Tools and Algorithms for the Construction and Analysis of Systems*, pages 337–340, Budapest, Hungary, 2008. Springer.
- [77] Ajaya K Swain and Valeria R Garza. Key factors in achieving service level agreements (sla) for information technology (it) incident resolution. *Information Systems Frontiers*, 25(2):819–834, 2023.
- [78] Hawraa Abdulameer Subeh and Ahmed Al-Ajeli. A learning classifier system for detection of service-level agreement violations in business process. In *2021 2nd Information Technology To Enhance e-learning and Other Application (IT-ELA)*, pages 40–45, Baghdad, Iraq, 2021. IEEE.
- [79] Xuezhi Zeng, Saurabh Garg, Mutaz Barika, Sanat Bista, Deepak Puthal, Albert Y Zomaya, and Rajiv Ranjan. Detection of sla violation for big data analytics applications in cloud. *IEEE Transactions on Computers*, 70(5):746–758, 2020.
- [80] Sudheer Kumar Battula, Saurabh Garg, Ranesh Naha, Muhammad Bilal Amin, Byeong Kang, and Erfan Aghasian. A blockchain-based framework for automatic sla management in fog computing environments. *The Journal of Supercomputing*, 78(15):16647–16677, 2022.
- [81] NK Neeraj, Aditya Nellikeri, P Varun, Santosh Reddy, Mangesh Shanbhag, Dg Narayan, and Altaf Husain. Service level agreement violation detection in multi-cloud environment using ethereum blockchain. In *2023 International Conference on Networking and Communications (ICNWC)*, pages 1–7, Chengalpattu, India, 2023. IEEE.
- [82] Ali Alzubaidi, Karan Mitra, Pankesh Patel, and Ellis Solaiman. A blockchain-based approach for assessing compliance with sla-guaranteed iot services. In *2020 IEEE International Conference on Smart Internet of Things (SmartIoT)*, pages 213–220, Tianjin, China, 2020. IEEE.
- [83] Rafael Brundo Uriarte, Huan Zhou, Kyriakos Kritikos, Zeshun Shi, Zhiming Zhao, and Rocco De Nicola. Distributed service-level agreement management with smart contracts and blockchain. *Concurrency and Computation: Practice and Experience*, 33(14):e5800, 2021.
- [84] Rohit Ranchal and Olivia Choudhury. Slam: A framework for sla management in multicloud ecosystem using blockchain. In *2020 IEEE Cloud Summit*, pages 33–38, Harrisburg, PA, 2020. IEEE.
- [85] Aditya Kumar Pandey, DG Narayan, and K Shivaraj. Sla violation detection and compensation in cloud environment using blockchain. In *2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, pages 1–6, Khargpur, India, 2021. IEEE.
- [86] PM Abhishek, Akash Chobari, and DG Narayan. Sla violation detection in multi-cloud environment using hyperledger fabric blockchain. In *2021 IEEE International Conference on Distributed Computing, VLSI, Electrical Circuits and Robotics (DISCOVER)*, pages 107–112, Nitte, India, 2021. IEEE.
- [87] João Paulo de Brito Gonçalves, Roberta Lima Gomes, Rodolfo da Silva Villaca, Esteban Municio, and Johann Marquez-Barja. A service level agreement verification system using blockchains. In *2020 IEEE 11th International conference on software engineering and service science (ICSESS)*, pages 541–544, Beijing, China, 2020. IEEE.
- [88] Amir Teshome Wonjiga, Sean Peisert, Louis Rilling, and Christine Morin. Blockchain as a trusted component in cloud sla verification. In *Proceedings of the 12th IEEE/ACM International Conference on Utility and Cloud Computing Companion*, pages 93–100, Auckland, New Zealand, 2019. ACM.
- [89] Huan Zhou, Cees de Laat, and Zhiming Zhao. Trustworthy cloud service level agreement enforcement with blockchain based smart contract. In *2018 IEEE International Conference on Cloud Computing Technology and Science (CloudCom)*, pages 255–260, Nicosia, Cyprus, 2018. IEEE.

- [90] Eder J Scheid, Bruno B Rodrigues, Lisandro Z Granville, and Burkhard Stiller. Enabling dynamic sla compensation using blockchain-based smart contracts. In *2019 IFIP/IEEE Symposium on Integrated Network and Service Management (IM)*, pages 53–61, Washington DC, USA, 2019. IEEE.
- [91] STA ENISA. Enisa, 2009.
- [92] Valentina Casola, Alessandra De Benedictis, Mădălina Eraşcu, Jolanda Modic, and Massimiliano Rak. Automatically enforcing security slas in the cloud. *IEEE Transactions on Services Computing*, 10(5):741–755, 2016.
- [93] Valentina Casola et al. Specs secure provisioning of cloud services based on sla management, 2013.
- [94] Valentina Casola, Alessandra De Benedictis, Massimiliano Rak, and Umberto Villano. A security metric catalogue for cloud applications. In *Complex, Intelligent, and Software Intensive Systems: Proceedings of the 11th International Conference on Complex, Intelligent, and Software Intensive Systems (CISIS-2017)*, pages 854–863, Torino, Italy, 2018. Springer.
- [95] Chun K Chan, Uma Chandrashekar, Steven H Richman, and S Rao Vasireddy. The role of slas in reducing vulnerabilities and recovering from disasters. *Bell Labs Technical Journal*, 9(2):189–203, 2004.
- [96] Cloud Security Alliance, Privacy Level Agreement Working Group . CSA: Privacy level agreement outline for the sale of cloud services in the european union. <https://cloudsecurityalliance.org/>, 2013. Tech. rep.
- [97] Michela D’Errico and Siani Pearson. Towards a formalised representation for the technical enforcement of privacy level agreements. In *2015 IEEE International Conference on Cloud Engineering*, pages 422–427, Tempe, AZ, USA, 2015. IEEE.
- [98] Vasiliki Diamantopoulou, Michalis Pavlidis, and Haralambos Mouratidis. Privacy level agreements for public administration information systems. In *CAiSE-Forum-DC*, pages 97–104, Essen, Germany, 2017. CEUR-WS.org.
- [99] Talal Halabi and Martine Bellaiche. A broker-based framework for standardization and management of cloud security-slas. *Computers & Security*, 75:59–71, 2018.
- [100] Amir Teshome, Louis Rilling, and Christine Morin. Verification for security monitoring slas in iaas clouds: The example of a network ids. In *NOMS 2018-2018 IEEE/IFIP Network Operations and Management Symposium*, pages 1–7, Taipei, Taiwan, 2018. IEEE.
- [101] Valentina Casola, Alessandra De Benedictis, Massimiliano Rak, and Umberto Villano. A novel security-by-design methodology: Modeling and assessing security by slas with a quantitative approach. *Journal of Systems and Software*, 163:110537, 2020.
- [102] Erkuden Rios, Marivi Higuero, Xabier Larrucea, Massimiliano Rak, Valentina Casola, and Eider Iturbe. Security and privacy service level agreement composition for internet of things systems on top of standard controls. *Computers & Electrical Engineering*, 98:107690, 2022.
- [103] Yudhistira Nugraha and Andrew Martin. Towards the classification of confidentiality capabilities in trustworthy service level agreements. In *2017 IEEE International Conference on Cloud Engineering (IC2E)*, pages 304–310, Vancouver, BC, 2017. IEEE.
- [104] Shengli Zhou, Lifa Wu, and Canghong Jin. A privacy-based sla violation detection model for the security of cloud computing. *China Communications*, 14(9):155–165, 2017.
- [105] Praveen Kumar Reddy Maddikunta, Quoc-Viet Pham, B Prabadevi, Natarajan Deepa, Kapal Dev, Thippa Reddy Gadekallu, Rukhsana Ruby, and Madhusanka Liyanage. Industry 5.0: A survey on enabling technologies and potential applications. *Journal of Industrial Information Integration*, 26:100257, 2022.
- [106] Shyam S Wagle. Cloud computing contracts: Regulatory issues and cloud service providers’ offers: An analysis. *Privacy and Identity Management. Facing up to Next Steps: 11th IFIP WG 9.2, 9.5, 9.6/11.7, 11.4, 11.6/SIG 9.2. 2 International Summer School, Karlstad, Sweden, August 21-26, 2016, Revised Selected Papers 11*, 7:182–198, 2016.