An Exploratory Study of Cloud Service Level Agreements - State of the Art Review

Saravanan K[1], Rajaram M[2]
[1] Department of Computer Science and Engineering, Anna University, Chennai
Regional Office, Tirunelveli, Tamilnadu, 627007 - INDIA
[e-mail: saravanan.krishnann@gmail.com]
[2] Department of Electrical Engineering Anna University, Chennai
Tamilnadu, 600025 - INDIA
[e-mail: rajaramgct@rediffmail.com]
*Corresponding author: Saravanan K

Received October 8, 2014; revised January 8,2014; accepted February 27, 2015;
published March 31, 2015

Abstract

Cloud computing evolve as a cost effective business model for IT companies to focus on their core business without perturbing on infrastructure related issues. Hence, major IT firms and Small & Medium Enterprises (SME) are adopting cloud services on rental basis from cloud providers. Cloud Service level agreements (SLA) act as a key liaison between consumers and providers on renting Anything as a Service (AaaS). Design of such an agreement must aim for greater profit to providers as well as assured availability of services to consumers. However in reality, cloud SLA is not satisfying the parties involved because of its inherent complex nature and issues. Also currently most of the agreements are unilateral to favour the provider. This study focuses on comprehensive, 360-degree survey on different aspects of the cloud service agreements. We detailed the life cycle of SLA based on negotiation, different types of SLA, current standards, languages & characteristics, metrics and issues involved in it. This study will help the cloud actors to understand and evaluate the agreements and to make firm decision on negotiation. The need for standardized, bilateral, semantic SLA has also been proposed.

Keywords: Cloud Service Level Agreements, SLA Life Cycle, SLA Negotiation, Types of Cloud SLA, SLA Characteristics, Semantic SLA.

http://dx.doi.org/10.3837/tiis.2015.03.001 **ISSN : 1976-7277**

1. Introduction

Service Level Agreement (SLA) is defined as a "documented agreement between the service provider and customer that identifies services and service targets" [1]. SLA documents are stated with different names – contractual agreement, master agreement, terms and conditions, Terms of Service (ToS), Acceptable User Policy (AUP), privacy policy, End User License Agreement (EULA), mutual contract [2]. Such SLA is composed of Service Level Objectives (SLO), which measures the quality of service by objective conditions or SLA parameters. Further it describes the roles and responsibilities of the consumer and provider. These SLOs differ by each provider and also by service models (SaaS, PaaS, IaaS) and deployment models (Public, Private, Hybrid), which have made SLA more intricate in nature. Here, the term consumer is used in generic to represent cloud users/customers/clients.

SLA is the fundamental facet of the cloud modeling, since cloud services are rented on pay-per-use. The advancement of cloud reduces the upfront investment of IT majors and enable service oriented market paradigm. Auto scale-out/scale-in ability of cloud changes the business culture and helps economics growth to the consumers ranging from personal, SME & corporates. Cloud TCO (Total Cost of Ownership) case study has explicitly stated that [3] adopting cloud solution about 10 years lifetime reduce $3 million dollars in TCO. SLA management is the umbrella activity that comes through the entire cloud life cycle. It should cover both the proactive (pre-negotiation) and reactive (post-negotiation) measurements. As the cloud services rely heavily upon seamless network, even a very minimal downtime will engender these services to become unavailable, thus impact the consumer's business agility. Also large IT corporates are moving towards cloud in order to reduce opex and capex costs [4]. For them, downtime of critical services reflects huge business loss. In the competitive cloud market, many providers offer the same services from SaaS through PaaS to IaaS, but each use different service definitions and metrics [5]. While choosing the services, consumers really need to have a sense of knowledge on these definitions and metrics. Hence formalized and competitive SLA which satisfies both the consumer and providers is essential.

From the consumer perspective, choosing the right provider using click-wrap agreements with expected services is the challenging task. Similarly from the provider side, offering different services to diversified users such as personal, SME & corporates is the big concern. Moreover, there are different devices used for accessing the cloud services such as desktop PC, laptop, tablet, kindle, mobile, etc. Also different adoptive approaches have been used for different services [4]. SME prefer the public IaaS services, since they can concentrate on their core business, leaving the infrastructure provisioning to cloud. There are several standards and practices proposed to define and structure the cloud SLA. Standards such as Cloud Industry Forum (CIF), Cloud Standard Customer Council (CSCC) & Cloud Select Industry Group (CSIG) and Open Cloud Computing Interface (OCCI) recommend the guidelines for drafting cloud SLA. Life cycle for an exemplary SLA contains drafting, negotiation, monitoring, violation, penalty enforcement

& renewal/exit conditions. Since the cloud SLA made by online click-through agreements, consumer is unaware of the hidden conditions in most of the occasions.
The rest of the study is organized as follows: Section 2 explores the related surveys and motivational factors of this study. Section 3 explains the SLA life cycle phases with respect to negotiation. Section 4 provides details about the SLA language specifications & standards and deals on different type of SLA for cloud services along with characteristics. Section 5 summarizes the service level objectives for assessing the cloud performance. Section 6 deals on the existing issues and future research directions in cloud agreements. Finally, section 7 gives the conclusion. We represented the various perspectives of cloud SLA explored over this study in **Fig. 1**.

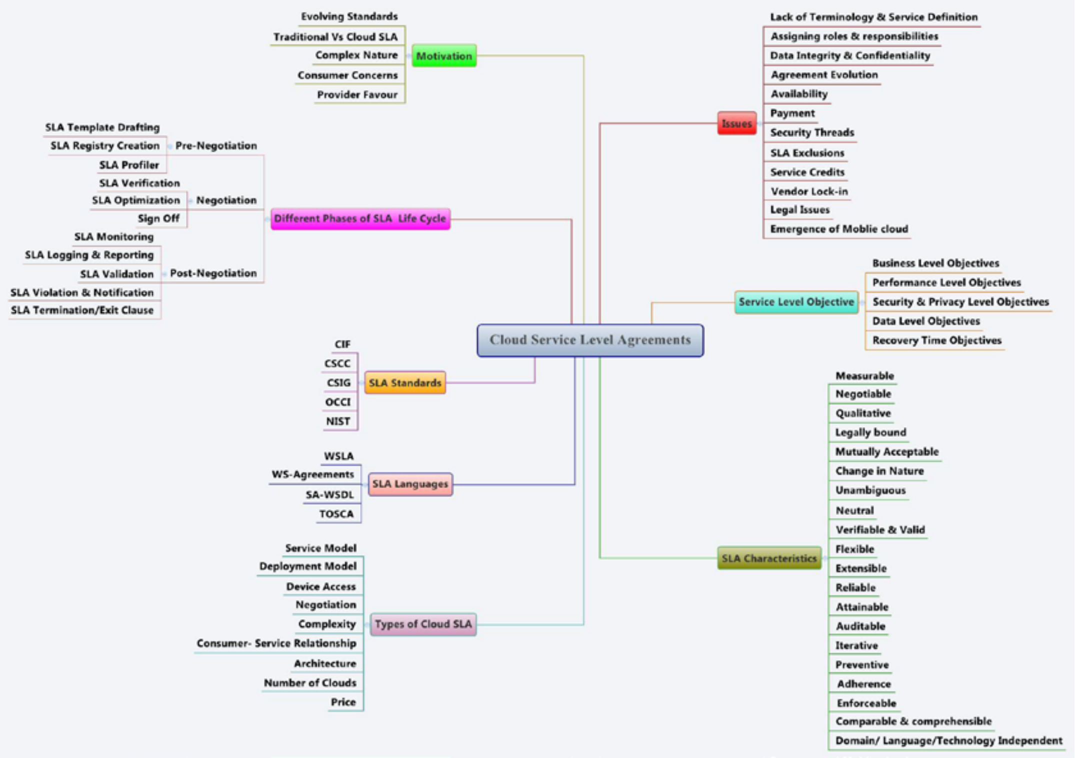

Fig. 1. Cloud SLA - Different Perspectives

2. Related Study and Motivation

Recently, studies and surveys are made in cloud SLA life cycle and its automation. A study proposed in anatomy of cloud SLA with six components [6] such as service guarantee, duration, granularity, exclusions, service credit and violation measurement & reporting. These components were compared in terms of compute and storage SLA of leading IaaS & PaaS providers. Another review illustrated [7] the formation of tailor-made SLA using pre- and post-interaction phases. In addition to that, several frameworks for SLA monitoring and violation prediction were listed for proactive SLA assurance. Another study surveyed [8] SLA models in the distributed domain environment (web services, grid & cloud). Major pitfalls in these models are also identified and narrated. Cloud taxonomy with eight SLA elements were proposed [9] and compared with IaaS, PaaS and web hosting providers. Besides, an extensive study of service agreements was made [10] in SLA Meta model along with the frameworks such as G-SLAM, SLA@SOI and EVEREST. Business use cases has also exemplified in this study. Nevertheless, it is apparent from these studies that neither cloud SLA standards & characteristics are explored nor the different types of SLA & SLO are detailed in depth so far. In this context, we propose a novel approach for cloud SLA life cycle in different perspectives and the types of SLA offered by cloud providers.

2.1 Motivation

Hence SLA plays a major role in the dynamic pricing model, price can be negotiated in the SLA signoff. Any disputes that arise between consumer and provider can be resolved by the SLA. In general, SLA agreements were signed by the senior IT and business decision-makers using on-screen, online form. The major factors for the motivation of this study are detailed below.

Evolving Standards - Currently, there is no standard nomenclature is used across cloud providers to define cloud service agreements and existing standards are not mature [6] [11, 12] enough to define the structure of the cloud SLA.

Traditional Vs Cloud SLA - Major difference between the traditional SLA and cloud SLA is that former uses the subscription/licence based model (fixed price) whereas the latter uses the pay-per use model (Dynamic price). SLA terms are more diligent in cloud on-demand business model, when compared with traditional SLA. Number of QoS parameters [13] is relatively more in cloud. Resource allocation on web services uses UDDI, whereas cloud uses dynamic virtual machine allocation strategy. SLAs for cloud has been analysed and differentiated against SLAs for web service & grid environment [8]. It emphasizes the different implementation approach for cloud SLA to integrate consumer business rules.

Complex Nature - Cloud SLA contains multi facet structures which result in many types of SLA and associated specific metrics on each of them. The different SLA considerations such as SLOs and KPIs for each service model and deployment model [14] have been listed out with respective metrics. For instance, IaaS SLA require compute, network and storage metrics whereas SaaS SLA require compositions of multiple metrics. Similarly, SaaS and PaaS SLA objectives are less precise than IaaS objectives. SLA structure may reusable in subsequent negotiation, but not the entire SLA.

Consumer Concerns - Cloud consumers are facing problems with understanding, selection, negotiation and access of non-interrupt services. Life cycle of SLA consists of diverse phases which require clear understanding. Consumer, the ultimate data owner, urges for control over the data and applications that reside on the cloud. Consumer Federation of America [15] has reported nine categories of cloud consumer concerns (Data use, Law enforcement access, Lock-in, Data security, Secondary uses of user data, Fairness in terms of service, Massive storage and massive failure, Jurisdiction and the role of transparency) with the recommendation consensus best practices for business adoption.

Providers Favour - CIF research [16] reveals that 78% of UK organisations use cloud services at present. But still user requirements are not satisfied by the cloud SLA [17]. We draw the attention to the fact that currently SLA violation post activities should be initiated by the user [14, 18] in a stipulated time frame in order to get the service credit for the failed service. There is no formal mechanism on how these service credits equalize sales/revenue loss in the user business [14]. If the service is inaccessible during business critical time, mere service credits no longer satisfy the cloud user. These situations become even worst in public cloud, since there is no strict violation policy. An automated configuration for SLA monitoring and violation detection has been proposed in SALMonADA [19] platform. Besides, best practices and cautions on public cloud provider's agreements were explored and raised queries on SLA penalties and service credit [14].

3. Different Phases of SLA Life Cycle

SLA Life cycle Metamodel [20] has been developed with the components such as service use, service modelling, SLA template definition, SLA instantiation and management, SLA enforcement and conclusion. BREIN project [21] has developed semantic SLA prototype with the actors namely SLA negotiator, User Agent, SLA Translator and Optimizer. Here, web ontology is used to translate the SLA terms in a common template.

Cloud actors defined by NIST (National Institute of Standards and Technology) [22] are: cloud consumer, cloud provider, cloud carrier, cloud broker and cloud auditor. The roles and responsibilities of each cloud actor should be clearly indicated as part of the SLA. e.g., cloud auditor can perform the independent assessment on deployed services to ensure security, privacy and performance. These roles might be combined or divided, depends on composition of the service. SLAs are drawn not only between consumer and provider; it can be an agreement between any two actors. Negotiation, provisioning, execution, assessment and termination constitute the SLA life cycle [23] in the dynamic pricing policy. It differs from the Metamodel [20] in the way that the creation of SLA template is considered as a predecessor of the lifecycle, but not being part of the lifecycle. Whilst SLA negotiation plays a vital role in dynamic price model deployed in private cloud, it is trivial for public cloud infrastructure services. IBM developed [24] the different states of SLA (SLA identified, SLA requested, SLA inactive, and SLA active, SLA terminated) and transitions between the states (Initial State, Request SLA, Approve

SLA request, Activate SLA, Terminate SLA) built using Unified Modeling Language (UML) model.

Based on the various approaches and contributions for SLA, we identified a novel cloud SLA life cycle phases in accordance with negotiation, which is denoted in Fig. 2. It can be classified as: Pre-Negotiation, Negotiation and Post-Negotiation.

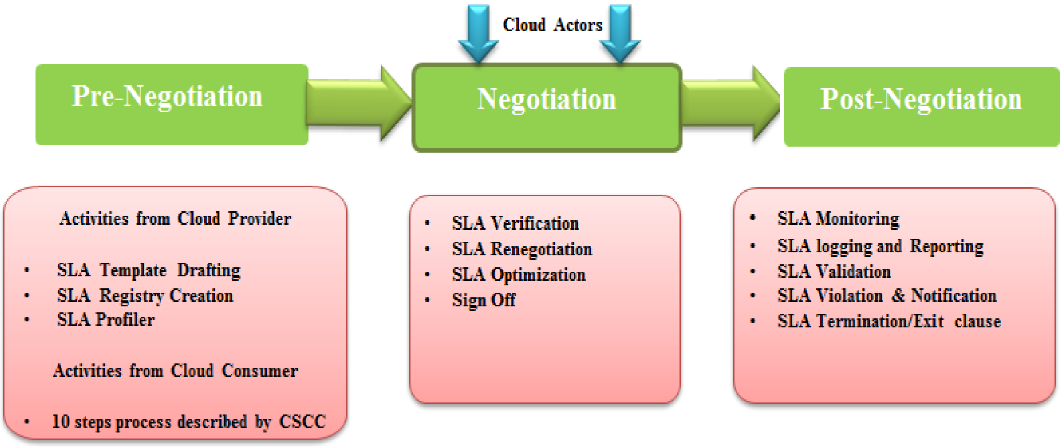

Fig. 2. Cloud SLA Life Cycle Phases

3.1 Pre-Negotiation

It involves the separate set of activities from both consumers and providers. SLA template formation and register into the cloud service repository are the pre-negotiation activities in the provider side. After that, consumers can access and evaluate these templates using profiler. The list of steps that consumer should consider for evaluating the SLA are constructed from the Cloud Standard Customer Council (CSCC)- Practical Guide to Service Level Agreements [14]. There are 10 steps for evaluating any type of cloud SLA and for comparing cloud providers.

Activities from the Cloud Provider:

3.1.1 SLA Template Drafting

Depending on the type of service, SLA template should be created. It should explicitly specify the SLOs with their KPI (Key Performance Indicator) metrics. These templates normally capture the non-functional requirements, leaving the functional requirements (service description) determined later during negotiation. The composition of functional and non-functional requirements makes each SLA unique. By default, cloud providers will made these templates publicly accessible in the web, so that individual/SME/corporate can download and compare with competent service providers. SLA templates are written in natural language [25] which is ambiguous to the consumers. Some providers left the technical terms unexplained which cause misperception to arrive the decision on SLA. e.g., Google BigQuery service agreements [26] specify that "Downtime means more than a five percent Error Rate. Downtime is measured based on server side error Rate". But, the calculation on the server side error rate depends on the back-off requirements which insists back-off interval of one second for each successive requests that actually further reduce the downtime. SLA general checklist (13 sections) [27] with contractual terms is proposed. This can be applied for SLA drafting to its completeness and proper structure.

3.1.2 SLA Registry Creation

SLA from different cloud providers for different services (service and deployment models) can be placed in a registry archive to enable effective advertisement of their services. Instead of searching the services in the provider's website, consumer can easily fetch it from the persistent SLA registry. Semantic annotation based cloud service repository [28] has been created to facilitate consumers to search for the indexed cloud services that they need.

3.1.3 SLA Profiler

SLA registry can be associated with profiler, which contains the analytic information of past service performance and historical data for every provider [29]. The outages happened, SLA breaches, successful negotiated services, penalty levels, number of certified cloud architects, cloud standards acquired and so on. It will aid the consumers in the vetting of the provider. It further helps the provider to envisage the future load & performance and gain reputation.

Activities from the Cloud Consumer:

It is imperative for the consumer to be aware of and understand the cloud SLA strategy and compare numerous providers SLA, before go for negotiation with specific provider. Pre-negotiation checklist for consumers defined by CSCC [14] contains constructive series of 10 steps, are summarized as follows.

1. Understand Roles and Responsibilities: Consumers should differentiate the cloud actors and their roles (defined in NIST) which are directly/indirectly involved in the SLA. Actors can be extended to further level depending on the number of vendors involved. Responsibilities of actors can be compromised and transferred to other actors during the negotiation.

2. Evaluate Business Level Policies: It includes data and business level policies, which can be clarified by the following questions asked by the consumer.

Data Policy: i) What are the cloud preservation strategy - backup, restore & integrity check?, ii) Which jurisdiction and law should follow, if data spans in several locations or in case of data theft/loss?, iii) How to verify the data location if auto-relocation policy exists? , iv) If SLA is terminated / expired, how long the data resides before consumer find alternative options?

Business Policy: i) What SLO metrics come under exclusions and why they excluded?, ii) What happens if the services are consumed beyond the SLA and how the charges will be? , iii) When will SLA get activated /enforced? e.g., immediately after signing the SLA or when the consumer accesses the service for the very first time?, iv)How to make the payment (Monthly/Quarterly/Yearly) or advanced reservation/on-demand ,auto-debit from the customer credit card, v) If there is any change in the services (add/ delete/update) ,then what is the impact in SLA ? , vi) What are the renewal policies exists -Auto renewal, bargaining mechanisms, vii) what are the different levels of support (based on severity/priority) by the provider for the production issues?, viii) What is the target time (Hours/Day/week) to resolve it?

3. Understand Service and Deployment Model Differences: KPI metrics offered by the different cloud services (IaaS /PaaS/SaaS) and deployment models (public/private/hybrid) are so different; hence the consumer must carefully choose the right service KPI. It is hard to generalize the SaaS metrics as there are ‘n’ numbers of unique applications exist worldwide.

4. Identify Critical Performance Objectives: Performance level metrics directly influence the business agility of the consumer. It includes the critical metrics such as availability and response time. Availability for various services (network, storage, application) has to be computed differently in the SLA.

5. Evaluate Security and Privacy Requirements: Security & Privacy metrics require continuous on-going progress in order to protect the consumer data against existing and new security threads. Security comprises of confidentiality, Integrity, authentication & access control mechanisms. Penetration test must be done independently by the consumer/agents to demonstrate the security capabilities of the provider. Cloud Security Alliance (CSA) [30] developed Consensus Assessments Initiative Questionnaire (CAIQ v3.0.1) to verify the security compliances of the cloud service models by the consumer/auditor. Likewise, privacy laws have been enforced for multiple countries & group people. Data privacy is ensured by the provider often using encryption key policies on the client data. The client who satisfies the access control for the files can view the decrypted data.

6. Identify Service Management Requirements: Consumers should be aware of the SLA management protocols such as auditing, monitoring, logging & reporting, accounting & metering and versioning after the agreements signed. e.g., metering possibly include the local VAT (Value Added Tax) accounted with the dynamic price. Continuous monitoring & reporting is required to assess the cloud service performance. Third party auditing at periodic intervals ensure the credibility of the client data. Addition/deletion/re-definition of services should undergo proper change & release control. Periodic patch updates of services should also be incorporated.

7. Prepare for Service Failure Management: Any service disruptions that impact the business trust-worthiness or liability of consumers can be treated as a SLA violation. Scheduled and unscheduled downtime which comes under SLA exclusions should be notified promptly to the consumer. This can be done in 2 ways. i) Fake transaction triggered from the consumer to ping the cloud for availability and response time. ii) Alert notification from the provider as part of SLA monitoring.

8. Understand the Disaster Recovery Plan: Consumers are still hesitant to adapt into cloud due to the unreliable disaster recovery process. Recovery Time Objectives (RTO) must have 'what-if' questionnaire in case of major disaster like Denial of Service (DoS) attacks, intrusion detection, network/server failure. e.g., RTO is crucial for mission critical applications which require 100% availability. Some providers even may assure 'cloud insurance' for the loss and failure.

9. Define an Effective Management Process: Preventive management policies should be placed to nurture the consumer-provider relationship. Review meetings promote the interaction between the consumer & provider and enhance the SLA procedures such as support, escalation and SLA changes. Feedbacks and opinions from the end user of the cloud application should also be incorporated. Rootcause analysis for frequent SLA misses helps the provider from paying the service credits and increases the confidence in cloud market.

10. Understand the Exit Process: Series of SLA breaches /violation without proper notification followed by service credits dissatisfy the consumer and exit of SLA. SLA ensures that exiting from cloud doesn't affect the consumer on-going business. How long the data is preserved till the consumer migrated/transferred to another provider? What is the format of data that could be extracted from cloud? Compatibility issues may arise. Consumer data can be expunged from cloud storage once the exit process is completed or the client made alternative storage.

3.2 Negotiation Phase

It's the acute phase since it leads to the final version of signed SLA, which is a living document. Many parties from either sides such as top business management, software architect, security experts, and finance & law experts are involved in the negotiation process, hence SLA encompasses all these aspects. Apart from these, cloud actors such as cloud carrier, cloud broker & auditor may also involve. This phase not applicable for non-negotiated agreements (Unilateral SLA) offered in public IaaS clouds. SME, the preferred customer of public IaaS, have no other option other than to accept the U-SLA [31, 32]. There are many approaches postulated for SLA negotiation.

C**loud4SOA** [33] have proposed a dynamic negotiation platform for PaaS providers. It provides interoperable heterogeneous framework for customized SLA negotiation with semantic description of services. **CONTRAIL** [34] is a multi-level SLA interaction model for federated cloud in which multiple IaaS providers are involved. SLA is spanned across the providers and is linked to offer a customized SLA. In order to achieve this, SLA splitting is used for convergence of multi-provider SLA. **IRMOS** project [35] introduced the dynamic SLA re-negotiation model, if the user/provider/application triggers any changes in the QoS terms during runtime. Re-negotiated agreements can be accepted or rejected depends upon the resources available in the server. **SLA@SOI** [36] addressed the entire SLA life cycle activities such as auto-negotiation, registry creation, monitoring, optimization, translation and SLAM (SLA Managers- consumer, provider and broker). It delivers the SLA-enabling reference architecture, which includes SLA translation and optimization.

3.2.1 SLA Verification

Negotiated agreement must be verified against its structure for completeness and correctness. Verification can be done with the help of SLA registry, in which registered pool of templates already exists. Missing of any SLO, which may significant to consumers, can be identified easily during verification. e.g., some providers [2, 37] are not liable for the data integrity policies in SLA.

3.2.2 SLA Renegotiation & Optimization

Renegotiation can be initiated either by consumer or provider, to incorporate the changes during runtime. Continuous improvement to optimize the performance of cloud services can be attained by the renegotiation of agreements. Number of times renegotiations triggered is depends on the factors such as changes in the SLO, organizational policy, violation, payment, etc. More optimal SLA is the primary thrust for renegotiation. Optimal might be in the form of profit, performance, consumer satisfaction or energy consumption. Negotiation and post-negotiation activities can be iterative to draft optimal SLA.

3.2.3 Sign Off

Once the consensus has been reached between consumer and provider, SLA would become live document till superseded by a revised version. Considered as a final activity in negotiation phase, signatories should ensure that SLA is validated in all aspects. Signed SLA should have the following attributes: Effective Date, Expiration Date, Version number & Signatories' details. Consumers must attempt prototype testing on the cloud to ensure the business functions. Currently, cloud SLA made with digital signature using online click through agreements.

3.3 Post-Negotiation

It encompasses the subsequent SLA management activities after provision and deployment of cloud services. SLA turns into real live engineer to monitor and assess the cloud.

3.3.1 SLA Monitoring

It is an automatic activity triggered immediately once SLA is signed. Consumers are more interested to see the higher level QoS metrics on the running services. Correlation should exist between the metrics and the higher level functional requirements [14]. These metrics are taken from the Virtual Machine (VM) instances at the regular intervals then processed by the SLA reporting module. If the consumer exceeds the maximum load (maximum number of concurrent on-line users; peak number of transactions per hour; or maximum number of concurrent user extracts), it leads to re-negotiation of SLA [38]. Providers employ monitoring services to extract the QoS data, but consumers may also engage third party monitoring tools such as Cloudstatus, Cloudkick for independent monitoring [39].

3.3.2 SLA Logging & Reporting

Multi-dimensional reports on every aspect of services should be presented to analyse the metrics. There are different type of cloud consumers exists from different domain (finance/marketing/sales/billing) and different levels (top management/security/software architect/support).Hence, reporting should excerpt and represent the different slices of the same data. Based on the QoS reports derived from cloud, preventive SLA violation mechanisms can be employed and renegotiation also be enforced to enable hierarchical self-healing of SLA. As the cloud data evolve huge in size (denoted in petabytes), BigData dimensions (volume, variety, velocity and veracity) can be used for future prediction of load and thus significantly reduce violation.

3.3.3 SLA Validation

Agreed service level of the providers should be validated against the QoS periodically to find any deficient in the service. Each SLO have the threshold value that helps to assess and compare with the current performance. High level business goals are validated in layered cloud to ensure trust and privacy [40].

3.3.4 SLA Violation & Notification

If any of the promised SLO has not fulfilled by the provider, then SLA is termed as violated, i.e., SLA slippage. (Sometimes, consumer may also violate the SLA by attempting vulnerability in the cloud service instances by accident). If SLA violated/missed by provider, consumers have to initiate the penalty claim consequences [41], which includes a tedious process flow.

1. Contact the providers support team for notification of service downtime. (Create a ticket based on severity) .It should be done within specific hours, e.g., 72 hours.
2. Submit a claim with evidence of violation such as detailed description, period of downtime, trace routes / log reports, escalation made to support team, service resume time and so on. Submission should be at the end of the billing period of services. e.g.,

Amazon AWS support centre facilitates the opening and tracking of ticket for production issues [42].

3. Validation of claim by providers with the help of logs at their end.
4. If the evidence supports the claim, provider pays the penalty to the failed services. These penalties normally given as service credits, which will be added with the service end period.

There are SLA exclusions specified in the SLA to favour the provider. It includes the following:

1. **Planned Maintenance:** Periodic hardware/software/network maintenance and troubleshooting activities in which consumers notifies in advance.
2. **Emergence Maintenance**: Unusual outages or failures happened in which prior notification cannot be done.
3. **Exclusions**: Force majeure, natural disasters, DoS attacks, internet downtime by third party network providers, wrong installation/configuration done by consumers. Emergency maintenance and exclusions are out of control to the providers.

3.3.5 Termination/Exit Clause

Consumer/ Provider may initiate the exit clause for the following reasons: 1. Agreement expired, 2. No more cloud service required for consumer, 3. Consumer goes for on-premise private cloud/ leaving from the cloud model/migrating to new cloud, 4. Provider goes out of business, 5.Consequence of SLA violation by either consumer or provider. Consumer data were normally retained in the cloud for specific period to allow the consumer for safer download and migration. This redemption period may vary by providers in respect to the data preservation policies. Providers are privileged to kill the VMs, removal of images and deletion of data. Different data purging approaches [2] are used by cloud providers. i) Data preserved for specific period (month/days), ii) Immediate deletion or iii) Customer own discretion.

3.4 Role of other Cloud Actors

Cloud Broker, otherwise termed as SLA Agent, plays in the pre-negotiation and negotiation phases. SLA agent varies with many types [43] – consumer agent, provider agent, negotiator, mediator, archiver and automatic service deployer. It acts as an intermediate, delegation entity for consumer as well as provider. In the pre-negotiation phase, consumer SLA agent matches the best SLA template that fulfils the consumer specifications by searching the registry and archives the historic QoS data of providers. In the negotiation phase, consumer and provider agents initiate the proposals across the multiple vendors and finalize the agreements. Price and Time slot based auto negotiation [44] has been implemented using cloud broker.

Cloud Carrier set up an internal SLA with cloud provider for the provisioning of cloud services to the consumer. Usually, network and telecommunication providers tied up with the provider agents for the secure connection and the end-end delivery of cloud services.

Interlinking among multiple carriers or in between any two actors is guaranteed over the carrier SLA.

Cloud Auditor, usually a third party agency, is employed to evaluate the security, privacy and performance on the deployed services. Auditing might be triggered as part of SLA monitoring and validation activities in the post-negotiation. Results of such auditing can be stored in the SLA profiler thus help the consumer agent in the selection of competent provider. Auditing ensure the standards compliance in the cloud and prevent regularity issues. Distributed auditing and logging mechanism implemented [45] for secure file access and revocation policies in cloud.

4. SLA Standards, Languages, Types and Characteristics

Various languages and standards used for specifying the service agreements and for defining the SLA operations. We tabulated these evolving standards and languages in **Table 1 & 2**. Also, Cloud SLA can be categorized based on the service model, deployment model, device access, negotiation, complexity, customer-service relationship and many more. SLA can differ based on geographical and juridical locations also. Scope of the SLA should mention which type it belongs to it. **Table 3** shows these different types of cloud SLA. Further, SLA structure has been divided into three characteristics [46] such as foundation elements, change management, and governance. Service level objectives and its content are specified in the foundation part .The uncertainty elements like future demand, change in the services and disaster plan are included in the change management. SLA violation, penalty, exit criteria dealt in the governance. We narrated the SLA characteristics in **Table 4**.

Table 1. SLA Standards

Cloud Industry Forum (CIF)	CIF implemented Code of Practice for cloud providers (CODE) [47] which includes three main classes namely A) Transparency, B) Capability and C) Accountability. Pricing policy, payment & termination terms, renewal process, and provision for customer migration should be specified in the CODE. The providers who satisfy the mentioned classes can be certified by CIF. It enables the cloud customers to search for the best provider agreements standardized by the CIF and also delivered the four steps buyer's guide for UK cloud consumers.
Cloud Standard Customer Council (CSCC)	CSCC, Non-standard organization with about 500 members, has delivered the practical guide for cloud computing [4] and cloud service agreements [14] along with use cases. It takes special care on domains such as financial, government, healthcare. Cloud security, XaaS and BigData also dealt by the CSCC working groups. It strives to motivate the deployment of cloud in the industries.

Cloud Select Industry Group (CSIG)	CSIG on service level agreements [5] is a working subgroup of - European Cloud Computing Strategy, operating towards the standards for European cloud industries. The eleven principles of SLA standards have been proposed. SLA can be set of documents - Master Service Agreement (MSA), Service Level Agreement, Service Agreement, Acceptable Use Policy, Privacy Policy, Security Policy, and Business Continuity Policy which describes the non-functional requirements and service description which describes the functional requirements of a specific service. It derives Service Level Objectives into four categories – Performance SLO, Security SLO, Data management SLO and Personal Data Protection SLO. Each SLO describes the set of terms to assess the cloud services. e.g., uptime/available time is calculated as "Total Possible Available Time-(Total Downtime-Maintenance Downtime)".
Open Cloud Computing Interface (OCCI)	OCCI [48] is the first protocol & API (supported by Open Grid Forum-OGF) for cloud standards such as integrity, portability, interoperability and extensibility. SLA@SOI is the implementation of OCCI, which provides a graphical editor to validate SLA templates. It uses JSON vocabulary for representing SLA, instead of conventional XML. It includes Java based rich APIs to automate the SLA life cycle and semantic based annotation model built using ontologies (OWL format).
Cloud Security Alliance (CSA)	CSA emphasise on security assurance of the providers. Implementation of Consensus Assessment Initiative Questionnaire (CAIQ) v3.0.1 with objective questions is used to assess the provider security SLO in depth [30]. Also Cloud Controls Matrix (CCM) v3.0.1 consisting of 16 control domains for security metrics mapped with equivalent standards worldwide. CSA also developed public registry STAR (The CSA Security, Trust and Assurance Registry) [49] which consists of four quality assessment levels (similar to CMM-Capability Maturity Model for software development) to certify the providers as per CAIQ & CCM. Cloud consumers may insist the providers for the STAR certification in the negotiation.
NIST	NIST developed the actor/ role based, vendor- neutral reference architecture for cloud computing. Standards Roadmap, a subgroup of NIST, developed standards maturity model with nine levels ranging from no standard to sunset [12]. This subgroup detailed the existing standards available for the SLA metrics – interoperability, portability, security, performance and accessibility.

Table 2. SLA Languages

Web Service Level Agreement	WSLA [50], a declarative XML schema based language, is used to specify negotiation, monitoring and notification of services [38].It allows for managing dynamically by runtime architecture and creating customized metrics in the form of resource and composite.

WS-Agreements	WS-Agreements from OGF [51], is another XML based specification language to orchestrate SLA life cycle. It consists of service terms (for service definitions) and guarantee terms (for conditions).It can be extended with WS-Policy, WS-Addressing, WS-Security, WS-Privacy standards. However, both WSLA and WS-Agreements lacks in domain vocabulary.
Semantic Annotations for WSDL and XML Schema (SA-WSDL)	SA-WSDL [52] is used for semantic specification of services. It can be represented by ontology and can be extended to any semantic mode i.e., annotations may be specified externally and embedded into other languages.
Topology and Orchestration Specification for Cloud Applications (TOSCA)	TOSCA from OASIS (a non-profit, open standards consortium) [53], is derived from XML vocabulary to describe the service templates in cloud. TOSCA metamodel includes the Node templates and relationship templates for defining the services. TOSCA grammar can be extended to vendor specific orchestration of services. Policy templates state the SLA quality metrics. Other languages used for the specifications are Web Service Offerings Language (WSOL) [54], SLAng [55], Quality of service Management Language (QML) [56], etc.

4.1 Types of Cloud SLA

Service Model: Each service model has its own metrics and hence agreements should be drafted specific to that model. Network and compute metrics included in the IaaS model whereas the data level metrics included in the storage model. PaaS production metrics should be stricter than PaaS development [14]. Similarly each SaaS has its own metrics specific to the application it hosts.

Deployment Model: As the public clouds are in 'Take it or Leave it' policy, negotiation normally excluded. People doubt on the security and privacy policies of the public cloud. Private SLA, both *on-site & outsourced models* needs more attention since it offers dynamic price and negotiable agreements. Also auto-renewal policy and performance metrics require consideration in the private. Community cloud SLA should focus on the business level policy that satisfies all the client organizations in the cloud.

Device Access: User interface of the devices differ based on the device we use. Mobile and kindle devices perhaps same, but desktop cloud application should be designed differently. Mobility metrics should be incorporated in the mobile applications as the user can access the cloud on the move. Primarily, SaaS platform should be modified for different devices since it control the application and user interface. Instance & operations of the application might be same, but the accessibility and user interface differ.

Negotiation: Off-the-Shelf agreements in which no negotiation done, are normally predefined by public clouds. They offer static, standard SLA which termed as U-SLA [32]. Roles and responsibilities of the parties involved normally not specified, hence it's a non-compromised. Conversely, Bilateral SLA (B-SLA) urges negotiation from both sides to reach mutual consent.

Complexity: Simple SLA is the straight-forward, single document that contains the structure of SLA. Multiple SLA spans with several agreements like privacy policy, acceptable user policy, security policy, business and data policy and so on. Heterogeneous deals about single customer/multiple customer provided with single/multiple service in single/multiple SLA by single/multiple providers. Depends on the number of cloud actors and vendors involved, SLA can be fine grained to multi-level.

Customer-Service Relationship: *Customer Based* - For individual customer and multiple service. *Service Based* - All customers using a single provider. *Multi-level SLA* - Same SLA satisfies the different aspects – corporate, customer and service [57].

Architecture: *Interconnection (Base layer) SLA*- Interconnections between the network providers, between application and network provider and between end-user and network provider. *Intra & Inter carrier Network Service (Middle layer) SLA*- The network intra-domain services & interconnections, inter-carrier network service interconnections agreements [58]. SLA for OSI layers model has been implemented in mPlane [59] in which service agreements of seven layers (layer 1-7) and their interface captured. *Application service (Top layer) SLA*-Network guaranteed application service.

Number of Clouds: Depends on the number of clouds (single/federated), agreements can be classified. Single sign-on access in federated cloud requires delegation services as part of SLA. The standards such as SAML, OAuth and OpenID [60] are used for this purpose.

Besides the above types, there are three SLA classes - Gold, Silver & Bronze SLA proposed based on the response time and arrival rate of the service requests [51]. Whilst gold SLA assures the response time, it is not guaranteed in the silver & bronze SLA. Cloud SLA must be capable of decoupled structure to accommodate the combination of these types.

Table 3. Types of Cloud SLA

Based on	Types
Service Model	SaaS, PaaS (Production/Development) , IaaS
Deployment Model	Public, Private(on-site /outsourced),Community, Hybrid(on-site private/on-site community/off-site private/off-site community or public)
Device Access	Desktop, Mobile, Kindle/Tablet/Notebook
Negotiation	Unilateral Vs. Bilateral
Complexity	Simple, Multiple, Multilevel (Carrier/Auditor/Broker internal SLA) , Heterogeneous (single/multiple consumer or provider, single/multiple service or SLA)
Customer-Service Relationship	Customer-based, Service-based, Multi-level based

Cloud Architecture	Interconnection (Base Layer SLA),Intra Network & Inter -Carrier Network (Middle Layer SLA) ,Application (Top Layer SLA)
Number of Clouds	Single Cloud Vs. Federated Cloud
Price	Category (Availability) - Gold (99.9%), Silver (99.5%), Bronze (99.0%)

4.2 Cloud SLA - Characteristics

Table 4. SLA Characteristics

Measurable	Contains the well-defined quantifiable SLOs and KPIs for each service
Negotiable (Re-Negotiable)	Pricing and KPI can be negotiated ; To optimize the SLA, re-negotiation enabled
Qualitative	Threshold levels for each SLO to ensure QoS; derived from metrics
Mutually Acceptable	By both the consumer and provider primarily; also for any two actors in the cloud
Change in Nature	Triggered by policy, price, contract period, etc.
Unambiguous	Each SLA terms should be unique and clear meaning
Verifiable & Valid	Verification as a pre-negotiation ; Validation as a post-negotiation
Legally Bound	Jurisdiction, litigation and privacy issues should be dealt lawfully
Comparable	KPI for each type of SLA can be compared with multiple providers
Comprehensible	SLA technical jargon should be comprehensive for business users
Neutral	Designed SLA not favouring to any specific cloud actor
Flexible	SLA template can be re-modified to accommodate changes
Extensible	Any cloud actor SLO can be added at runtime
Reliable	Ensures the efficiency & accuracy of service delivery in the form of SLOs
Iterative	SLA life cycle activities can be repeatable; granular to multi-level internally in service/cloud actor.
Preventive	Prevent violation, termination and security issues
Auditable	Internal/Third party auditing for validation of service
Adherence	Compliance with consumer's and provider's organizational and business policies
Attainable	SLA KPI threshold must be achievable

Enforceable	Renegotiation,violation,penalty claim and termination can be enforceable
Domain/Language/Technology Independence	Independent to domain(web services, grid and cloud), Language (WSLA, WS-Agreements, SA-WSDL) ,Technology (frameworks / architectures / vendor lock-in software)

5. Service Level Objectives (SLO)

In general, cloud Metrics are associated with the SLO such as business level objectives, performance level objectives, security & privacy level objectives, data level objectives and recovery time objectives [5, 14]. Qualitative metrics are derived from quantitative metrics, which are the explicit results from cloud monitoring.

Business Level Objectives (BLO) usually drafted and managed by the top business management of the consumer. Here, core importance is given for SLA management, not for QoS. i.e., management aspects of the SLA such as pricing & payment, penalty level & escalation level support, renewal & termination policy, application migration/transfer , SLA exclusions, governance & legal issues, standards & certification from regularities. Business level objectives must ensure that client organizational business model should not be convinced /deviated by SLA.

Performance Level Objectives (PLO) are the KPI for assessing cloud application/network/storage quality. It varies by deployment models and service models. But, some of the metrics are common to all. e.g., availability and response time metrics are included invariably in the performance reports. These metrics hold high visibility among cloud providers hence it gave the competitive edge over the others. Also any minor variation in the SLO leads to violation. Infrastructure Response Time (IRT) can be considered as a key performance metric for computing IaaS availability [61].

Security & Privacy Level Objectives (S&PLO) ensure the three metrics CIA (Confidentiality, Integrity and Availability). Besides, security SLOs includes metrics for authentication, authorization, cryptography, auditability and vulnerability [5]. These metrics are interrelated e.g., auditability requires third party authentication incorporated. Cloud storage access and revocation policies using Attribute/Role based encryption can be employed for authorization. Promising more reliable cloud service is the primary goal of security. CSA STAR certification detailed the security practices of various cloud providers and made it publicly available to compare the security SLOs [49]. Cloud security factors in managerial, physical and technical areas were identified and compared [62] with the priority given by the different enterprises model.

Data Level Objectives (DLO): Several SLOs used for data level SLO such as data mirroring, backup & restore, data retention & deletion and data transfer rate. CAIQ v3.0.1 [30] provides a list of questions to assess the data governance policies. Specific metrics such as data I/O rate, frequency of backup, retention limit in size and time and weak/strong deletion. The composite metrics such as data portability, durability, preservation, remanence, liability and integrity can also be derived.

Recovery Time Objectives (RTO): Metrics in compliance with the disaster recovery plan are defined here. The maximum downtime of service disruption for critical and non-critical business functions should be identified and agreed in the SLA. Mean Recovery Time is used to compute RTO. It is a preventive mechanism that comprises of 'What-if' questions for force majeure activities.

6. Current Issues and Future Directions in Cloud SLA Life cycle

6.1 Current Issues in Cloud SLA Life cycle

SLA, primarily an agreement that should satisfy both the parties involved, is not reflecting sprit of relationship between them in cloud. The more standardized and customizable SLA needed. In this section, the issues in different phases of life cycle are described.

6.1.1 Issues in Pre-Negotiation

Lack of Terminology and Service Definitions: Some of the terms defined in the agreement are ambiguous resulting misunderstanding between consumer and provider. e.g., Legal terms are specifically more ambiguous. As cloud SLA is still evolving and yet to be standardized, vague terms make more complex.

Assigning Roles and Responsibilities: Hence multiple & multilevel layers as well as actors involved in cloud model, clear delineation required for the roles they play and responsibility they have been assigned. Failure/disrupts in the vendor services will not be violation since providers is not liable for it. Cloud application is a composition of services, since sub-contractors involved between multiple services should be identified.

6.1.2 Issues in Negotiation

Data Integrity and Confidentiality: Responsibility of encryption, backup & archival of the data has been forced to consumer end [2], leaving the liability from provider end. Patch updates of the software will also part of it. Some providers charges for integrity, considering as an additional service, not an integral part of data storage [2].Another study stated that [63] information are non- confidential, which means data can be disclosed. Social networking applications moving into the cloud contains huge user generated content consist of personal details. These details should not be disclosed .Data retention and deletion policy for cloud should be standardized. Data remanence enforces the assured deletion of data from the providers. In present scenarios, providers won't liable for data loss/theft and it is the liability of consumers [30]. Providers can only compensate for the disrupted service. Indirect liability such as revenue/reputation loss is also concern for the consumer. e.g., Zoho [64], provider of PaaS and SaaS services, stated in their terms that no liable for incidental, indirect and punitive damages or loss of business profit.

Agreement Evolution: Most of the providers can make amendments in their SLA from time to time without/with notification (Some providers post the recent versioning in their website and some others inform by email). If the consumer continuously uses the service after the change, it is deemed to be considered as an accepted SLA. Whilst signing of SLA involves consent of both parties, changes not bother about it. SLA review should not be unilateral and must be endorsed by all the stakeholders.

Availability: Cloud providers offer availability in 'Nines', ranging from 1 to 7. Even it is more for the storage availability. Monthly downtime of services can range from 0.259 seconds for 7 nines (99.99999%) and 72 hours for single nine (90%) [65]. Based on the price of services, availability also varies. 99.5% - 'silver' class; 99.9% - 'gold' class by BizCloud private-cloud service [66]. But how the availability is calculated is still an issue. Providers include the uptime of 12 months when start using the service, which postulate the actual percentage of downtime. ENISA Survey [67] illustrated that only 15% received the availability reports from the public cloud.

Payment: SLA act differently for paid and free services. Provider can terminate the free account (includes deletion of consumer data) without further notice, if it was inactive for ninety days. For paid services, non-payment of account will cease the services and remove the data. Upon termination of SLA, data would be kept in cloud for specific grace period and consumer should pay for the retrieval of data, after the grace time. [2]. Dynamic price model enforces different payment for the same services. Unused payment that should be returned to the consumer will take maximum grace period.

6.1.3 Issues in Post-Negotiation

Security Threads: As cloud services accessed through internet, security attacks are very common. It takes any one of the vulnerability – phishing, skimming, eavesdropping, SQL injection, Cross Site Scripting, DNS attacks, Denial of Service or malware (Virus /Trojan/Worm).These threats have been categorized as basic, network level, application level & data level [68]. Also, security issues for different service models (SaaS/PaaS/IaaS) [69] have to be dealt in distinct manner. To identify the security weakness, penetration test can be performed independently by consumer. But only 14% regular penetration tests were conducted and 7% received the reports [67].

SLA Exclusions: Besides the planned downtime, there are exclusions (unplanned maintenance and force majeure) beyond the control of the providers. But, only few consumers knew penalty exclusions, e.g., 22% reported in the ENISA survey [67]. As each provider can have their own exclusions specification, it is the liability of the consumers to act on service disruptions. Even the providers assuring 100 % availability till have the exclusions [2]. Providers reserve the right to suspend the service at any time. Zoho [64] terminate the unpaid inactive accounts over 4 months.

Service Credits: Notification of service credit request in IaaS cloud is done by the consumers, which makes cumbersome activities [41]. Compensation for SLA violation would be in terms of service credits i.e., extension of service in future contracts. It indirectly forces the agreements to be extended in order to utilize the service credits. Maximum of service credits normally not exceed customer monthly payment (upto 30% in Amazon & HP for availability <99.0%; upto 50% in Google for availability <95.0%) [26, 42, 70]. But there won't be any scale for maximum threshold for down time. Moreover, Service credits are given only for baseline services affected in unplanned downtime, not for the planned outages and exclusions category. Some of the providers, for instance Amazon EC2 [42] will not credit if the service credit is very low e.g., less than $1 USD. Setting up the maximum & minimum for service credits and downtime is still an issue. If there is more than one cloud service denied for consumers, claim can be made for only one service.

Vendor Lock-in: Currently the cloud SLA indirectly forcing the consumers to be dependent on the vendor [71]. During the termination of agreement the following issues arise:

1. Customer business data resides in the providers place. How to move/migrate/delete/purge the data which are redundant, multi jurisdictions & vendor specific formats and compatibility. e.g., SaaS provider Salesforce returns the data to consumer in CSV format [31].
2. Limited portability/interoperability of client applications & data migrating from one provider to another with minimal effort and cost.
3. Fear on business continuity makes the consumer a chaotic decision on break of SLA.
4. Usability of cloud services through user interfaces made difficult to assimilate new environment.

The compatibility and interoperability of applications and data, specified in the SLA, must be properly examined to avoid vendor-lock in.

Legal Issues: Many providers offer Availability Zone (AZ) for data redundancy. As cloud enables anywhere, anytime access of storage, when the dispute arose, it's the burden for consumer to seek which jurisdiction laws to be imposed. Amazon asks the consumers during negotiation to select the zone to resolve the legal issues [2]. Claim notification and disputes should be sought within short span of time, which make it difficult for consumers. For instance, major providers such as Amazon EC2, HP and Rackspace stated in their SLA [42, 70, 72] that consumer must notify the violation in 30 days. Law enforcement agencies face forensic challenges when issue arise on privacy of cloud data [73].AUP differ by nation and application and deny the use of cloud in any one of the illegal form. Unaware of these policies will result serious legal actions against consumer. Transmission of junk/spam mails done by accident will result termination of services [2].Usually, providers design service agreements in such a way that to avoid litigation from their side. e.g., most providers [26, 42, 69, 72] such as Google, Amazon, HP and Rackspace mentioned the force majeure events in broad terms.

Emergence of Mobile Cloud: Access of cloud services using mobile and handheld devices is exponentially increasing as it provides on the move usage. But, mobility metrics are still not matured enough to standardize. Besides, it leads to some issues [68] - confidentiality of data sharing, dynamic network monitoring and scalability and access control & identity management.

6.2 Future Research Directions in Cloud SLA Life Cycle

There are several supporting frameworks proposed for the automation / semi-automation of the SLA life cycle activities. We examined & compared such frameworks and their automation level (manual/semi-automatic/automatic) based on the negotiation and summarized in **Table 5**. Activities such as SLA registry, profiling, consumer pre-negotiation steps and verification are requiring automation and are done manually. With the help of open source and commercial platforms, most providers automated the SLA monitoring and reporting. The different Service Level Objectives associated with each phase also specified. It is interesting to note that most of the frameworks work in a specific life cycle activity, requiring semantic relationship in between them.

Table 5. SLA Activities – Automation level and Standards

Cloud SLA Life Cycle Activities	Automation level	Supporting Frameworks	SLO
Pre Negotiation			BLO
SLA Template Drafting	Semi-automatic	EGI - SLA for Research community [20]	
		Cloud TM - Custom SLA templates [20]	
		ETICS - Flexible SLA template for business models [58]	
		BREIN - Semantic Annotation of SLA [21] [28]	
SLA Registry Creation	Manual	CSA STAR - Provider Certification [49]	
		CIF CODE - Provider Certification [47]	
SLA Profiler	Manual	ASAPM project - Profiler [29]	
CSCC 10 Steps Guidelines	Manual	CSCC standards for Cloud SLA [14]	
Negotiation		OPTIMIS ,cloud4SOA- Dynamic Negotiations [20]	SPLO , DLO
SLA Verification	Manual	IRMOS - Mapping [35]	
SLA Renegotiation	Semi-automatic	IRMOS - Dynamic Renegotiation [35]	
		MODAClouds - Runtime Renegotiation	

		[20]	
SLA Optimization	Semi-automatic	SLA@SOI - Optimization [36]	
		Cloud TM - Self-Optimization [20]	
Post-Negotiation			
SLA Monitoring ,Logging and Reporting	Automatic	Open Source and Commercial Cloud Monitoring platforms [39],SLA@SOI [36]	PLO, SPLO
SLA Validation	Semi-automatic	Proactive Validation [40]	
SLA Violation & Notification	Semi-automatic	SALMonADA [19] ,VISION Cloud - Proactive SLA Violation Detection [20]	RTO, DLO
Termination/Exit Clause	Semi-automatic	WSAG [51]	

Based on the issues and automation frameworks, we listed the future research directions in the SLA life cycle.

Pre-Negotiation: Customized SLA templates for each type of cloud and consumer business model are still challenging and require much attention. SLA registries such as CSA-STAR and CIF-CODE are yet to be adopted by providers and linked with profiler framework for effective vendor-neutral lookup services. Profiler can also be effectively used for dynamic pricing of cloud resources. A knowledge-based Continuous Double Auction (CDA) model was used to fix the price in cloud market based on the historical data [74]. CSCC's guidelines for evaluating agreements may be modelled to review the SLA in a procedural way. Currently, no cloud SLA template tailored with complete specifications satisfying the cloud actor's requirements. Hence, novel agreements design has to be established with the right mix of SLO & KPI using the SLA languages.

Negotiation: Though many systems developed for dynamic SLA negotiation, participation of cloud actors is limited. Hence, negotiating platform involving actors (external and internal) is vital in cloud model. As cloud is more dynamic than web services and grid, renegotiation model must handle the unexpected changes after deploy. Reverse engineering can be applied to optimize and re-negotiate SLA. Building trust relationship among cloud actors is also required as part of the negotiation. e.g., cloud auditing in federated cloud cannot be possible without trust. Trust transmission mechanism using IBC-Based Entity Authentication Protocols was proposed in federated cloud environment [75]. Prototypes for strong linkage between negotiation and service execution are mandatory to resolve inconsistencies in runtime.

Post-Negotiation: Role of SLA in cloud migration from one provider to another yet to be explored. Insight research is essential on compromised service credits that convince all the cloud actors. Consumer payments to cloud services are done by auto-debit. Similarly, auto-credit for disrupted services during SLA violation can be configured to eliminate complex penalty claim procedure. Several unknown scenarios exist in the sequence of SLA monitoring to termination. Moreover, SLA escalation process can be redesigned to be proactive, instead of reactive.

7. Conclusion

This study analysed several aspects of cloud service level agreements. The sequence of activities in the SLA negotiation life cycle has been identified & narrated. Emerging standards for SLA and languages also detailed. Different types of SLA have been identified based on service/deployment model, device access, architecture and numbers of clouds. We further listed out the issues in service agreements which needs research focus. It is evident from the study that standardized & user-centric SLA is the up-thrust for the cloud consumers. With the help of the semantic technologies such as Web Ontology Language (OWL), Resource Description Framework (RDF), Extensible Markup Language (XML) & Web Service Modeling Ontology (WSMO) design of SLA can be done in meaningful way i.e., moving from syntax (structured) to semantics (comprehensible). Discovery, ranking and management of services using semantic SLA have been identified already [76]. As SLA establishes the relationship between two set of peoples, conflicts always exists. It can be resolved by adopting the semantic knowledge in the formation of SLA. We proposed to do the following:

1. Development of customizable, user centric semantic SLA using the web 3.0 languages.
2. Semantic discovery for search and retrieval of service level agreements using annotated service descriptions from providers registry based on the user innate.
3. Automation of SLA life cycle activities by building ontologies for each phase of the SLA.

References

[1] ISO/IEC 20000-1:2011, "Information technology-Service management-Part 1: Service management system requirements". Article (CrossRef Link)

[2] Bradshaw. S, Millard. C and Walden. I, "Contracts for clouds: a comparative analysis of terms and conditions for cloud computing services," *Int. J. Law Inf. Technol.* vol. 19, no**.** 3, 187–223, 2011. Article (CrossRef Link)

[3] "A Case Study of Cloud Development, Time to Value and Total Cost of Ownership," *Cloud TCO Case Study*, 2012. http://cloud-perspectives.com/woodward-temp/June2012-Cloud-TCO-Case-PDF.pdf

[4] Cloud Standards Customer Council, "Practical Guide to Cloud computing version 2.0," 2014. http://www.cloudstandardscustomercouncil.org/PG2CC_v2.pdf.

[5] Cloud Select Industry Group, "Cloud Service Level Agreement Standardisation Guidelines," 2014. http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?action=display&doc_id=6138.

[6] Baset and Salman A, “Cloud SLAs: present and future,” *ACM SIGOPS Operating Systems Review* vol. 46, no. 2, 57-66, 2012. Article (CrossRef Link)

[7] Sun. Le, Jaipal Singh, and Omar Khadeer Hussain, “Service level agreement (SLA) assurance for cloud services: a survey from a transactional risk perspective,” in *Proc. of 10th International Conference on Advances in Mobile Computing & Multimedia*, pp. 263-266, ACM, 2012. Article (CrossRef Link)

[8] Alhamad, Mohammed, Tharam Dillon and Elizabeth Chang, “Service level agreement for distributed services: a review,” in *Proc. of Dependable, Autonomic and Secure Computing (DASC), 2011 IEEE Ninth International Conference on*, pp. 1051-1054, IEEE, 2011. Article (CrossRef Link)

[9] Prodan, Radu, and Simon Ostermann, “A survey and taxonomy of infrastructure as a service and web hosting cloud providers,” in *Proc. of Grid Computing, 2009 10th IEEE/ACM International Conference on*, pp. 17-25, IEEE, 2009. Article (CrossRef Link)

[10] Wieder, Philipp, Joe M. Butler, Wolfgang Theilmann and Ramin Yahyapour, “Service level agreements for cloud computing,” Springer, 2011. Article (CrossRef Link)

[11] European Telecommunications Standards Institute (ETSI), “Cloud Standards Coordination,” 2013. Article (CrossRef Link)

[12] NIST Cloud Computing Standards Roadmap Working Group, “NIST Cloud Computing Standards Roadmap Version 2,” 2013. Article (CrossRef Link)

[13] Wu. L, Buyya. R, “Service Level Agreement (SLA) in utility computing systems,” *Techniques and Research Directions IGI Global*, USA 2011. Article (CrossRef Link)

[14] “The CSCC Practical Guide to Cloud Service Level Agreements v1.0,” *Cloud Standards Cust omer Council*, 2012. http://www.cloudstandardscustomercouncil.org/2012_Practical_Guide_to_Cloud_SLAs.pdf

[15] Hoofnagle, Chris Jay, “Consumer Protection in Cloud Computing Services: Recommendation s for Best Practices from a Consumer Federation of America Retreat on Cloud Computing,” 3 0, 2010. Article (CrossRef Link)

[16] Cloud Industry Forum, “The Normalisation of Cloud in a Hybrid IT Market-UK Cloud Adopt ion Snapshot & Trends for 2015,” 2014. http://cloudindustryforum.org/downloads/whitepapers/CIF_WP_14.pdf

[17] White Paper- “Take Back Control of Your Cloud Apps: Which SLAs Really Protect Your Bottom Line?,” *Compuware APM*, 2013. Article (CrossRef Link)

[18] L. Badger, "NIST Draft Special Publication 800-146, DRAFT Cloud Computing Synopsis and Recommendations," *National Institute of Standards and Technology*, 2011. http://csrc.nist.gov/publications/drafts/800-146/Draft-NIST-SP800-146.pdf

[19] Muller. C, Oriol. M, Franch. X, Marco. J, Resinas. M, Ruiz-Cortes. A and Rodriguez. M, “Comprehensive Explanation of SLA Violations at Runtime,” *IEEE Transactions on Services Computing*, vol. 7, no. 2, pp. 168-183, 2014. Article (CrossRef Link)

[20] Kyriazis.D, “Cloud computing service level agreements–exploitation of research results,” *Technical report*, *European Commission*, Brussels, 2013. Article (CrossRef Link)

[21] B. Koller, H. Munoz Frutos and G. Laria G, “Service Level Agreements in BREIN,” *Springer Grids and Service-Oriented Architectures for Service Level Agreements, Springer*, 2010. Article (CrossRef Link)

[22] F. Liu, J. Tong, J. Mao, R. Bohn, J. Messina, L. Badger, and D. Leaf, “NIST Cloud Computin g Reference Architecture (NIST SP 500-292),” *National Institute of Standards and Technolog y*, U.S. Department of Commerce, 2011. http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909505

[23] P. Hasselmeyer, B. Koller, I. Kotsiopoulos, D. Kuo and M. Parkin, "Negotiating SLAs with Dynamic Pricing Policies," in *Proc. of SOC@ Inside'07*, 2007.

[24] N.Hargrove, "Service Lifecycle Governance with IBM WebSphere Service Registry and Rep ository SG24-7793-00," *IBM Redbooks*, 2009. http://www.redbooks.ibm.com/redbooks/pdfs/sg247793.pdf

[25] Stahl, Elisabeth, "Performance and Capacity Themes for Cloud Computing," *IBM Redbooks*, 2013. http://www.redbooks.ibm.com/redpapers/pdfs/redp4876.pdf

[26] Google Cloud Storage, Google Prediction API, and Google BigQuery SLA, 2014. https://cloud.google.com/bigquery/sla.

[27] J.Vandendriessche and F.Coppens, "Checklist: Cloud Computing Agreements v1.3," 2013. http://www.crosslaw.be/checklist-cloud-computing-agreements/

[28] Rodríguez-García, Miguel Ángel, "Ontology-based annotation and retrieval of services in the cloud," *Knowledge-Based Systems*, vol. 56, pp. 15-25, 2014. Article (CrossRef Link)

[29] He, Qiang, "Lifetime service level agreement management with autonomous agents for services provision," *Information Sciences* 179.15: 2591-2605, 2009. Article (CrossRef Link)

[30] Cloud Security Alliance - Consensus Assessments Initiative Questionnaire v3.0.1 (CAIQ), 2014. https://cloudsecurityalliance.org/research/cai/

[31] W.K. Hon, C. Millard and I. Walden, "Negotiating Cloud Contracts: Looking at Clouds from Both Sides Now," *Stanford Technology Law Review*, vol. 16, no. 1, 2012. Article (CrossRef Link)

[32] Comuzzi, Marco, Guus Jacobs, and Paul Grefen, "Clearing the Sky-Understanding SLA Elements in Cloud Computing," *Beta Working Paper series 412*. http://cms.ieis.tue.nl/beta/files/workingpapers/wp_412.pdf

[33] Kamateri, Eleni, "Cloud4SOA: A Semantic-Interoperability PaaS Solution for Multi-cloud Platform Management and Portability," *Service-Oriented and Cloud Computing*, Springer Berlin Heidelberg, 64-78, 2013. Article (CrossRef Link)

[34] R. Cascella, L. Blasi, Y. Jegou, M. Coppola, C. Morin, "Contrail: Distributed Application Deployment under SLA in Federated Heterogeneous Clouds," *Springer, Lecture Notes in Computer Science*, 2013. Article (CrossRef Link)

[35] T. Cucinotta, F. Checconi, G. Kousiouris, D. Kyriazis, T. Varvarigou, A. Mazzetti, Z. Zlatev, J. Papay, M. Boniface, S. Berger, D. Lamp, T. Voith and M. Stein, "Virtualized e-Learning with Real-Time Guarantees on the IRMOS Platform," *IEEE International Conference on Service-Oriented Computing and Applications, SOCA2010*, Perth, 2010. Article (CrossRef Link)

[36] W. Theilmann, J. Lambea, F. Brosch, S. Guinea, P. Chronz, F. Torelli, J. Kennedy, M. Nolan, G. Zacco, G. Spanoudakis, M. Stopar, G. Armellin, "SLA@SOI Final Report," 2011. http://sla-at-soi.eu/wp-content/uploads/2008/12/SLA@SOI-FinalReport.pdf

[37] AWS Service Terms, http://aws.amazon.com/service-terms/, 2014.

[38] B. Kevin and D. Hanf, "Cloud SLA Considerations for the Government Consumer," *Cloud Computing*, 2010.Article (CrossRef Link)

[39] G. Aceto, A. Botta, W. De Donato, and A. Pescape, "Cloud Monitoring: A Survey," *Computer Networks*, vol. 57, no. 9, pp. 2093-2115, 2013. Article (CrossRef Link)

[40] Haq, Irfan Ul, Ivona Brandic, and Erich Schikuta. "SLA validation in layered cloud infrastructures," *Economics of Grids, Clouds, Systems, and Services, Springer Berlin Heidelberg*, pp, 153-164, 2010. Article (CrossRef Link)

[41] Service Level Agreement documentation for Microsoft Azure Web Sites SLA, 2015. http://www.microsoft.com/en-us/download/details.aspx?id=39303

[42] Amazon EC2 Service Level Agreements, 2015. http://aws.amazon.com/ec2/sla/
[43] Venticinque, Salvatore, R. Aversa, B. D Martino, M. Rak, and D. Petcu, "A cloud agency for SLA negotiation and management," in *Proc. of Euro-Par 2010 Parallel Processing Workshops*, pp. 587-594, 2011. Article (CrossRef Link)
[44] Son, Seokho and K. M Sim, "A Price-and-Time-Slot-Negotiation Mechanism for Cloud Service Reservations," *Systems, Man, and Cybernetics, Part B: Cybernetics, IEEE Transactions on*, vol. 42, no. 3, pp. 713-728, 2012. Article (CrossRef Link)
[45] R. Nishana, and K. Saravanan, "Secured Image Sharing and Deletion in the Cloud Storage Using Access Policies," *International Journal on Computer Science and Engineering*, vol. 5, no. 4, pp. 230-237, 2013.
[46] Goo, Jahyun, "The role of service level agreements in relational management of information technology outsourcing: an empirical study," *Management Information Systems Quarterly*, vol. 33, no. 1, 2009. http://aisel.aisnet.org/cgi/viewcontent.cgi?article=2786&context=misq
[47] Cloud Industry Forum-Code of Practice for Cloud Service Providers v1.0, 2013. http://cloudindustryforum.org/component/content/article?id=43
[48] Open Cloud Computing Interface. http://www.occi-wg.org/about/
[49] Cloud Security Alliance-Security, Trust and Assurance Registry (STAR), 2014. https://cloudsecurityalliance.org/star/
[50] Keller, Alexander and Heiko Ludwig, "The WSLA framework: Specifying and monitoring service level agreements for web services," *Journal of Network and Systems Management*, vol. 11, no. 1, pp. 57-81, 2003. Article (CrossRef Link)
[51] Andrieux, A., et al., "Web Services Agreement Specification (WS-Agreement) GFD-RP," 2007. http://www.ogf.org/documents/GFD.107.pdf
[52] Semantic Annotations for WSDL and XML Schema -W3C Recommendation, 2007. http://www.w3.org/TR/2007/REC-sawsdl-20070828/
[53] Topology and Orchestration Specification for Cloud Applications Version 1.0, *OASIS Standard*, 2013. http://docs.oasis-open.org/tosca/TOSCA/v1.0/os/TOSCA-v1.0-os.html
[54] Tosic, Vladimir, Kruti Patel and Bernard Pagurek, "WSOL—Web Service Offerings Language," *Web Services, E-Business, and the Semantic Web*, pp. 57-67, 2002. Article (CrossRef Link)
[55] Lamanna, D. Davide, James Skene and Wolfgang Emmerich, "SLAng: a language for service level agreements," pp. 100-106, 2003. http://discovery.ucl.ac.uk/721/1/9.9.6slang.pdf
[56] Frølund, Svend, and Jari Koistinen. Qm, "A language for quality of service specification," *Hewlett-Packard Laboratories*, 1998. http://hpassethub.designory.com/techreports/98/HPL-98-10.pdf
[57] OGC, "Official Introduction to the ITIL Service Lifecycle," Stationary Office Books, 2007.
[58] ETICS project, Deliverable D4.1, "End-to-end service specification template," https://bscw.ict-etics.eu/pub/bscw.cgi/d19910/D4.1%20End-to-End%20service%20specification%20template.pdf
[59] mPlane – An Intelligent Measurement Plane for Future Network and Application Management. http://www.ict-mplane.eu/
[60] Murukutla, Pratap and K. C. Shet, "Single Sign on for Cloud," in *Proc. of Computing Sciences (ICCS), 2012 International Conference on*. IEEE, 2012. Article (CrossRef Link)
[61] V.Vineetha, "Performance monitoring in cloud," *Infosys Ltd*, 2012. Article (CrossRef Link)
[62] Y. B Yoon, J. Oh and B. G Lee, "The Establishment of Security Strategies for Introducing Cloud Computing," *KSII Transactions on Internet and Information Systems*, vol. 7, no. 4, 2013. Article (CrossRef Link)

[63] Reed, Chris, “Information Ownership in the Cloud,” *Queen Mary School of Law Legal Studies Research Paper* 45, 2010. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1562461

[64] Zoho Corporation Service Level Agreements, 2014. http://www.zoho.com/terms.html

[65] Comparing Public Cloud Service Level Agreements –White paper, *Dimension Data*, 2013. Article (CrossRef Link)

[66] BizCloud VPE Service Descriptions Summary, http://assets1.csc.com/cloud/downloads/8051_14_BizCloud_VPE_Service_Offering_2_6_18.pdf

[67] Dekker, M., and G. Hogben, “Survey and analysis of security parameters in cloud SLAs across the European public sector,” 2011. *Article (CrossRef Link).*

[68] Bhadauria, Rohit, “A survey on security issues in cloud computing,” *arXiv preprint arXiv*, pp. 1109.5388, 2011. http://www.chinacloud.cn/upload/2011-10/11100221191648.pdf

[69] S. Subashini and V. Kavitha, “A survey on security issues in service delivery models of cloud computing,” *Journal of Network and Computer Applications*, vol. 34, pp. 1-11, 2011. Article (CrossRef Link)

[70] HP Compute Cloud Service Level Agreements, 2015. http://www.hpcloud.com/sla/compute

[71] Torode, C, “Beware These Risks of Cloud Computing, from no SLAs to Vendor Lock,” *CIO News*, 2009. Article (CrossRef Link)

[72] Rackspace Cloud Service Level Agreements, 2014. http://www.rackspace.com/information/legal/cloud/sla

[73] I. Walden, “Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent,” *Queen Mary University of London, School of Law*, 2011. Article (CrossRef Link)

[74] S. Shifeng, J. Jiang, Y. Wu, G. Yang and W. Zheng, “A knowledge-based continuous double auction model for cloud market,” in *Proc. of Semantics Knowledge and Grid (SKG), IEEE 2010 Sixth International Conference on*, pp. 129-134, 2010. Article (CrossRef Link)

[75] C. Cao, R. Zhang, M. Zhang and Y. Yang, “IBC-Based Entity Authentication Protocols for Federated Cloud Systems,” *KSII Transactions on Internet and Information Systems*, vol. 7, no. 5, 2013. Article (CrossRef Link)

[76] Dastjerdi, A. Vahid, S. G. H Tabatabaei and R. Buyya, “A dependency-aware ontology-based approach for deploying service level agreement monitoring services in Cloud,” *Software: Practice and Experience*, vol. 42, no. 4, pp. 501-518, 2012. Article (CrossRef Link)

Mr.K.Saravanan, is working as an Assistant professor, Department of Computer Science & Engineering at Regional Office, Anna University, Tirunelveli. He received his master degree in M.E Software Engineering in 2007 and B.E degree in Computer Science & Engineering. His research interest includes Cloud computing, Software engineering, Web Technology and Semantic Web. He published papers in 8 international conferences and 11 international journals.

Dr.M.Rajaram received his B.E. degree in Electrical and Electronics Engineering in 1981 and M.E. degree in Power Systems in 1988. Besides having a strong technical expertise and analytical skills, he received his Ph.D degree in 1994. He has contributed to the areas of Computer Networks, High Voltage Engineering, Measurement and Instrumentation, Adaptive Controller, Electro Magnetic Theory and Distributed Computing. He has 157 publications in renowned research journals, 111 research publications in International Conferences, 73 research publications in National Conferences, more than 100 technical reports and six technical books some of which he has co-authored. Currently, he is the Vice-Chancellor of Anna University, Chennai.