Cloud Computing : Service Level Agreements(SLA)

A.S.Rumale, Dr. D. N. Chaudhari

Abstract— Cloud computing is a very complex system. It involves integration of many Information Communication Technologies, like Internet, Distributed Computing, Grids, Client- Server, etc. . . Main issue with any cloud is user's trust. To achieve this user-trust many solutions are put forth by scientists one of which is service- usage agreement based cloud development. In this system cloud service provider and user makes some agreement regarding services of cloud with its usage; generally termed as Service Level Agreements(SLA). SLA usually documents the legal and technical issues related with usage of cloud by users. As developing and maintaining a cloud involves a good amount of finances, many time users find themselves in no condition to argue with cloud provider; or, to force it to bend its working as per user's requirement. User, in such cases generally accepts a most suitable SLA package from the cloud service provider. So it's necessary for user to what is SLA? What it should have to talk about? And, why it is difficult to impose users perspective on cloud service providers for SLA based Cloud? This paper explores some desired features of SLA with challenges in implementing a SLA based cloud to answer above questions upto some extent.

Index Terms— Cloud computing, Service level agreements(SLA), IaaS, PaaS, SaaS, SLA issues

1 Service Level Agreements :Introduction

Service Level Agreements(SLA), plays a very important role in cloud operations, as cloud computing need to take care of many non-technical issues like local legal issues, business contract between cloud provider and user. Security and depth of security thus can be forced by the proper SLA[1]. In practice monitoring/verifying that SLA levels are respected by cloud-provider is difficult because it is usually the case that there is no opportunity to negotiate the contents of the agreement with the major cloud providers like Amazon, google etc. They offer a standard set of terms and conditions and user generally have no power to force SLA-based security terms and conditions on the major providers. But, this approach can be used when implementing a private cloud. This won't cancel the significance of SLA based security in cloud, as many major providers already have a SLA based security drafts with below discussed features of SLA. Figure 1 briefs out some salient points to consider while drafting SLA to make cloud more secure and trusted. Following issues makes SLA an important part of cloud computing.

(i) **Integration:** Cloud need to look for integration points with security and identity management technologies you already have, such as Active Directory, and controls for role-based access and entity-level applications. A proper integration promises better performance. Integration and its way need to be documented and agreed upon by the cloud provider as well as users for reliable implementation and constructing test benches for cloud computing services and security depth. Security depth means the type and extent of security measures that can be used to secure the cloud and its services.[1], [2]

(ii) **Privacy:** A cloud service must includes data encryption, effective data anonymization, and mobile location privacy. This is essential to be mentioned in SLA, as SLA gives a blueprint for what to add and what to deduct for providing privacy to user. Privacy means whatever communication that happens through cloud among cloud users must not be made public; and no data of any user will be available to anyone without the concerned users permission. Privacy providing mechanisms must need to obey the law and order or legacy system of the country of cloud provider as well as country of the cloud user; and that by not offending any international laws. Thus an ill documented SLA and privacy system implemented based on it can legally jeopardize the cloud provider and user.[2], [3]

(iii) **Identity and access:** A Cloud must have a means of preventing inadvertent access. cloud more often uses Internet for connectivity, which is having its own list of security threats. One risk of using Internet is the possibility of identity hijacking or theft. This, if not properly handled in SLA as well as in implementation, then the user may get compromised by some Cybergoon. A mechanism strong enough to safeguard the users account by not allowing any inadvertent access to it is desired. This can be achieved by using multilevel

- *A S Rumale is currently pursuing Doctora; program in cloud computing in SGBA University, Maharashtra, India. E-mail: arumale@gmail.com*
- *Dr. D. N. Chaudhari, is academic dean and professor at JDIET Yavatmal E-mail: dnchaudhari2007@rediffmail.com*

user authentication process and dynamic password generation with SSL(Secure Socket Layer) or like protocols. In authors view a VPN(Virtual Private Network) with right mix of multilevel authentication process can help to solve this to some extent.[2], [3]

(iv) **Compliance :** Cloud must have vendor certification and compliance with industry and government standards that affect users agency. As mentioned in above point ii, cloud need to obey the legacy systems, both global and local for not to legally offend any party either cloud provider or cloud user. A total compliance with Industry and Governments can only make a cloud a success story.[4]

(v) **Service integrity:** Cloud must protect software from corruption (malicious or accidental) and always ensure the security of the written code.This can be explained using the concept of using Electricity; When plugging an electric appliance into an outlet, One care neither how electric power is generated nor how it gets to that outlet. This is possible because electricity is virtualized; i.e., it is readily available from a wall socket that hides power generation stations and a huge distribution grid. When extended to information technologies, this concept means delivering useful functions while hiding how their internals work. Cloud Computing itself, to be considered fully virtualized [5], must allow computers to be built from distributed components such as processing, storage, data, and software resources. Thus, Cloud Computing in its simplest meaning is an advanced client-Server mechanism with Service Oriented Architecture(SOA)[6], where server provides services to client and client(clouduser) pay the charges for them to server(Cloud-serviceprovider). This simply mean any corruption in any component or part or service of a cloud can kill the very purpose of the the cloud. So, protecting the cloud components becomes a first priority for service integrity. This can be achieved by employing redundancy principle (keeping at least one exact uptodate copy of whatever data/code is there on the cloud ; and providing a atleast one robust exact copy of the hardware/machines with same software(s) to carry out the work incase of failure of either). This also involves providing proper cooling and ventilation to heating cloud(servers) serving the users. Service integrity thus can be considered as soul of the cloud computing and a must part of any SLA.[2]

(vi) **Jurisdiction:** The location of a cloud providers operations can affect the privacy laws that apply to the data it hosts.Does users data need to reside within users legal jurisdiction? Governments records management and disposal laws may limit the ability of agencies to store official records in the cloud[7]. We already discussed this in above points ii and iv. Apart from the above, the principles of cloud (refer table I) itself require stringent SLA implementation. Table I points out that SLA must mentioned the way of resource pooling, virtualization, providing reliability and availability through elasticity and automation, and the measures to charge per use of a service, that is, billing schemes. Just mentioning these in SLA are not sufficient. It requires continuous monitoring and correct implementation of SLA. Thus, we can that SLA plays very important role in secure cloud computing. SLA in every term provides details of design and implications of the implemented design; and proper implementation of SLA promises a secure and reliable Cloud to work with[1-3],[8].

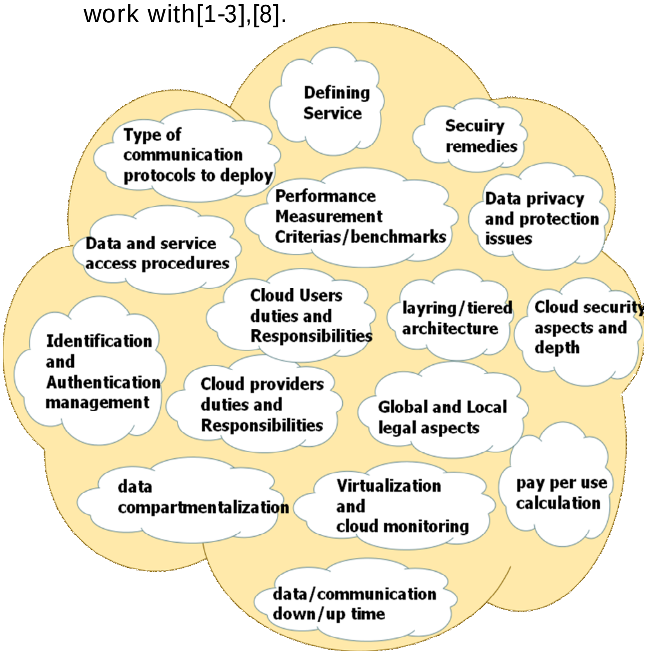
Defining Service
Type of communication protocols to deploy
Secuiry remedies
Performance Measurement Criterias/benchmarks
Data privacy and protection issues
Data and service access procedures
Cloud Users duties and Responsibilities
layring/tiered architecture
Cloud security aspects and depth
Identification and Authentication management
Cloud providers duties and Responsibilities
Global and Local legal aspects
data compartmentalization
Virtualization and cloud monitoring
pay per use calculation
data/communication down/up time

Fig. 1. Salient points to consider while drafting SLA

2 Salient Points of SLA

Figure 1 depicted some salient features of SLA. In this section all those points/features are discussed in brief. Defining Service : Defining service(s) offered by cloud help in implementing the service(s) in correct way. A service can be termed as any technical computation or legal necessities carried out by

CSP(Cloud Service Provider) strictly on users request. Such service carried out by CSP may be chargeable or free. It is desirable that, any service must not have to become chargeable unless it is fully committed; i.e. Acknowledged by the user. But this can unnecessarily congest the network. This simply suggests that while defining service(s) one must have to think billing independent of service(s).

TABLE I
FIVE MAIN PRINCIPLES OF CLOUD COMPUTING

Resource	Explanation
Pooled resources	Resources like Infrastructures, Platforms, and Services are gathered and made available to any subscribing users.
Virtualization	High utilization of hardware assets or resources as none of them remain ideal because many subscribing users can use them at any given point in time.
Elasticity	Due to Distributed Nature and SOA of Cloud computing; Cloud Computing enables user as well as service providers to add/remove any user/resource to/from the cloud dynamically without affecting its working.
Automation	Build, deploy, configure, provision, and move, all resources without manual intervention
Metered billing	Per-usage business model; pay only for what one use

Metered billing: Improper billing is never welcomed; and so it is required to consider many factors for billing. Few billing approaches are discussed below.

per minute billing Billing starts with logging in of user in cloud. A pre-agreed charge per minute is used by cloud-usage-monitor program to calculate the bill. Bill won't consider whether user used any service of cloud or not. The billing process is simple, start with login and ends with logout. Whatever the time span in minutes is multiplied with the simple pre-agreed charge to get the bill. Problem arises if user's terminal fails after login making logging out difficult. In such case a wrong bill may get calculated. This can be avoided by periodically checking whether user is active or not by sending some blank message to client. If client won't response within a specific time; it automatically get logged out by the system.

per usage billing Billing starts if and only if client uses some service(s) of cloud with pre-agreed charges(may differs with each service and charges may be usage time based or fixed per service). For ideal time when logged in user is not using the cloud a pre-agreed fix charge is added. Because, such an ideal user actually remain active in resource-allocation queue, and required to be served immediately with its request for a service(s).

fixed billing Billing in this case is generally fixed for some maximum usage. Maximum usage limit is set high enough so that client rarely touch it. Incase client crosses the maximum usage limit; one of the above billing criteria may get used by CSP for after maximum-usage usage of the cloud service. Example: Say $ ####.## fixed per month(year or some term) for maximum usage traffic M GB. For any usage less than or equal to M GB the bill is fixed to $ ####.## , and for any usage X greater than M, bill for (X-M) usage is calculated using one of the above two methods or any other agreed method in SLA. Fixed billing is the most popular billing method among CSP's and users. Implementing Proper billing criteria independently for individual client is very difficult; because, it increases the complexity of the cloud-usage-monitor system. To avoid the complex monitoring for billing system, CSPs generally came ups with pre-designed billing modules, and client(s) need to choose one out of them.

Type of communication protocols to deploy : Poorly designed communication protocols used or cloud computing can act as bottleneck for efficient performance. The existing protocol suit with some modification as per the clouds requirement is generally used. For secure communication between cloud user(s) and CSP, SLA must have to concretely define the communication and trust model. Trust here means complete security and privacy of users data; wherever it is in cloud. We suggested the three tier protocol architecture [9] for this, refer figure2. SLA must talk on it; as proper communication protocols ensure contention and congestion free network.

Performance Measurement criteria/benchmarks : Deciding on performance measurement criteria or benchmarks is very essential to achieve and maintain the right performance. These should be flexible enough to change with advent in technologies used. Data and service access procedures : Creating proper user hierarchy for data and service access is one of many points in SLA implementation. These procedures decides on different access rights to different users with user centric billing.

Data privacy and protection : Data Privacy plays very important role when data is on cloud. Data privacy ensures Trust among cloud providers and users. Data can be attacked or hacked either by programs or by persons. A strict security mechanism required to be implemented to protect data from inadvertent access or attacks. SLA documentation plays important role of providing directions for this.

Data compartmentalization : Every cloud users data and operations require to be handled separately with different adress spaces allotted to every user. This ensures that no user can intervene or modify or read other users data or operation inadvertently. A proper documentation on what is required in compartmentalization can result in better system. This also includes the data distribution and retrieval strategies. A good data compartmentalization of data ensures better performance with more trust.

Data communication up/down time : All cloud based solutions relays heavily on Internet(Intranet, incase of private cloud), and slow up/down time of net can create unnecessary delays. Deciding proper strategies for high performance is very necessary.

Layered architecture : Layered architecture as shown in figure2 promises efficient and dynamic execution of the programs and services by distributing functionality. Security aspects and depth : Security aspects stands for how to provide security to cloud; while Security depth is directly concern with the implementation details for security mechanisms. This can be moderate to strict depending upon type of data and operation a user tends to carry on the cloud. For data, usually public and not-so-important(not having any attachment as of financial type or some information which if get leaked can cause financial or personal hazards) security can be kept at moderate level.

Security remedies : Cloud is used 24_7 by many users and hence there is always possibility of an error(s) or security breach(es) that might happen. Remedies are precautions taken to minimize such possibility. IAM : Identity & Access Management in cloud can be seen as a separate system and required to be drafted and implemented with utmost care so that virtually no, and practically negligible inadvertent access of cloud can be possible. It is always difficult to achieve a fool-proof
system due to some non technical limitations.

Virtualization and monitoring : A great deal of efforts are required for virtualization, as cloud uses it very heavily. Continuous monitoring of the system for security threats, billing and other operations can only result in good cloud. Directives on what, why, and how to monitor; must part
of SLA.

Users duties and responsibilities : Many usage problems are there which can not be solved using technology; an ethical behaviour of user is assumed in such cases and required to be drafted and reminded to users periodically. Providers duties and responsibility : Many usage problems are there which can not be solved using technology; an ethical behaviour of provider is assumed in such cases and required to be drafted and reminded to providers periodically. Global/Local legal aspects : These may be technical or non technical, and required to be handled accordingly.

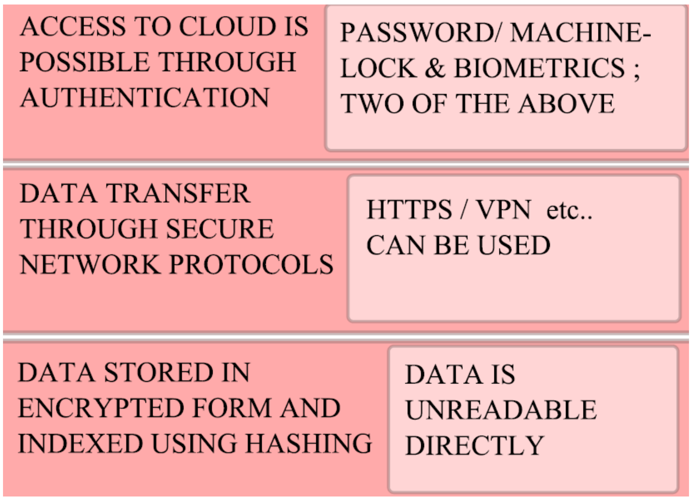
ACCESS TO CLOUD IS POSSIBLE THROUGH AUTHENTICATION
PASSWORD/ MACHINE-LOCK & BIOMETRICS ; TWO OF THE ABOVE
DATA TRANSFER THROUGH SECURE NETWORK PROTOCOLS
HTTPS / VPN etc.. CAN BE USED
DATA STORED IN ENCRYPTED FORM AND INDEXED USING HASHING
DATA IS UNREADABLE DIRECTLY

Fig. 2. 3-tier communication architecture for Cloud-Computing[9]

3 Challenges In Having User-SLA for Cloud

User-SLA, here mean SLA drafted by user based on which CSPs provides their services. The main challenge we are not having yet such User-SLA based cloud is due to economically weak condition of user compare to CSP. This condition may includes lack of knowledge and expertise required to implement and maintain cloud services, lack of resources available to user, and no-unity in users spread over a globe with insufficient funds to build cloud. Another hurdle in having a user-SLA is legal aspects. Each country has her own laws to which a business owner(here in this case CSP) need to abide by. Client(s) also need to obey the rules of their own country with the rules of CSP's. International laws also plays an important role in drafting of such SLAs. Usually no user like to go through all such legal complexities and so try to choose most approximate SLA from CSP(SLA that are more nearer to users perspectives and needs) for cloud services.

4 Conclusion

We will like to say that though there is need for user defined SLA based cloud; It is unlikely to have such user-SLA based cloud due to (a) complex nature of such cloud, as for each user it plays using different SLA, (b) economically weak condition and non-unity of user(s) to force such user-SLA on CSP, and (c) hesitation of user(s) in going through all legal details required to draft such SLAs.But, may be in near future we will see such user-SLA based clouds, and more fine SLAs; mean while every cloud user must have to analyze the SLA provided by CSP before accepting it.

References

[1] G. Jacobs, "Clearing the Sky in Cloud Computing: a Framework for SLA Elements in the Cloud. ," Series Master Theses Operations Management and Logistics, School of Industrial Engineering, Eindhoven University of Technology, February 2012.

[2] D. M. Dekker and D. G. Hogben, "Survey and analysis of security parameters in cloud SLAs across the European public sector ," European Network and Information Security Agency (ENISA), survey report, December 2011, pp. 1-36. [Online]. Available: http://www.enisa.europa.eu

[3] B. Ludwig and S. Coetzee, "Implications of security mechanisms and Service Level Agreements (SLAs) of Platform as a Service (PaaS) clouds for geoprocessing services," Applied Geomatics, Springer, pp. 1–13, 2012. [Online]. Available: http://dx.doi.org/10.1007/s12518G012G00083G3*

[4] P. Patel, A. Ranabahu, and A. Sheth, "Service level agreement in cloud computing," pp. 1–10, 2010-11. [5] "Cloud Computing Security : Making Virtual Machines Cloud-Ready ," a Trend Micro White Paper May 2010, pp. 1-12.

[6] ASP-Team, Cloud Computing Certification Kit Specialist : Software as a service and Web Applications: The art of Service. The Art of Service Pty Ltd, 2011, pp. 1-219.

[7] Andrew Geyer, Melinda McLellan and Hunton Williams LLP, "Strategies for Evaluating Cloud Computing Agreements," BloombergFinanceL.P., BloombergLawReportsTechnologyLaw, 2011, pp. 1-4.

[8] N. R. Putri and M. C. Mganga, "Enhancing Information Security in Cloud Computing Services using SLA Based Metrics ," Master Thesis ,Computer Science , Thesis no: MCS-2011-03, School of Computing , Blekinge Institute of Technology , SE 371 79 Karlskrona, Sweden, January 2011.

[9] A.S.Rumale and Dr.D.N.Chaudhari, "Cloud computing : Designing secure storage- cloud system," International Journal Of Computer Science And Applications, ISSN: 0974-1003, vol. 4, no. 3, pp. 120–124, Oct-Dec

2011.