Emerging Security Issues in Cloud Computing Environment for Enforcing Service Level Agreement

[1]Mr. N. Jayapandian
M.E.,(Ph.D)
Assistant Professor
Knowledge Institute of Technology,
Salem.

[2]Dr. A. M. J. Md. Zubair Rahman
M.S.,Ph.D,
Assistant Professor
Knowledge Institute of Technology, Salem.

[3]R. B. Sangavee
PG Scholar,
Knowledge Institute of Technology,
Salem.

[4]S. Radhikadevi
PG Scholar,
Knowledge Institute of Technology,
Salem.

Abstract-Cloud computing that provides cheap and pay-as-you-go computing resources are rapidly gaining momentum as an alternative to traditional IT Infrastructure. As more and more consumers delegate their tasks to cloud providers, Service Level Agreements (SLA) between consumers and providers emerge as a key aspect. Due to the dynamic nature of the cloud, continuous monitoring on Quality of Service (QoS) attributes is necessary to enforce SLAs. Also numerous other factors such as trust (on the cloud provider) come into consideration, particularly for enterprise customers that may outsource its critical data. This complex nature of the cloud landscape warrants a sophisticated means of managing SLAs. This paper proposes a mechanism for managing SLAs in a cloud computing environment using the Web Service Level Agreement(WSLA) framework, developed for SLA monitoring and SLA enforcement in a Service Oriented Architecture (SOA). We use the third party support feature of WSLA to delegate monitoring and enforcement tasks to other entities in order to solve the trust issues. We also present a real world use case to validate our proposal. The cloud computing uses the internet as the communication media. When we look at the security of data in the cloud computing, the vendor has to provide some assurance in service level agreements (SLA) to convince the customer on security issues. Organizations use cloud computing as a Service infrastructure; critically like to examine the security and confidentiality issues for their business critical insensitive applications. Yet, guaranteeing the security of corporate data in the "cloud" is difficult, if not impossible, as they provide different services like Software as a service (SaaS), Platform as a service (PaaS), and Infrastructure as a service (IaaS). Each service has their own security issues. So the SLA has to describe different levels of security and their complexity based on the services to make the customer understand the security policies that are being implemented. There has to be a standardized way to prepare the SLA irrespective to the providers. This can help some of the enterprises to look forward in using the cloud services. In this paper, we put forward some security issues that have to be included in SLA.

Keywords: Cloud Computing, SLA, SaaS.

1. INTRODUCTION

Cloud computing is the new trend of computing where readily available com- puting resources are exposed as a service. These computing resources are gen- erally offered as pay-as-you-go plans and hence have become attractive to cost conscious customers. Apart from the cost, cloud computing also supports the growing concerns of carbon emissions and environmental impact since the cloud advocates better management of resources. We see a growing trend of off-loading the previously in-house service systems to the cloud, based primarily on the cost and the maintenance burden. Such a move allows businesses to focus on their core competencies and not burden themselves with back office operations.[2]

Cloud Computing has evolved through a number of implementations which include application service provision (ASP), grid and utility computing, and Software as a Service (SaaS). But the overarching concept of delivering computing resources through a global network is rooted in the sixties. The idea of an "intergalactic computer network" was introduced in the sixties by J.C.R. Licklider, who was responsible for enabling the development of ARPANET (Advanced Research Projects Agency Network) in 1969.His vision was for everyone on the globe to be interconnected and accessing programs and data at any site, from anywhere. The clouds have different architecture based on the services they provide. The data is stored on to centralized location called data centers having a large size of data storage. The data as well as processing is somewhere on servers. So, the clients have to trust the provider on the availability as well as data security. The SLA is the only legal agreement between the service provider and client. The only means the provider can gain trust of client is through the SLA, so it has to be standardize. In this paper, section two describes the service level agreement, section three explain present SLA's of cloud computing, and section four discusses how to standardize SLA's followed by the proposed data security issues.

2. THE SERVICE LEVEL AGREEMENT

A service level agreement is a document which defines the relationship between two parties: the provider and the recipient. This is clearly an extremely important item of documentation for both parties. If used properly it should:

1.1 Identify and define the customer's needs

1.2 Provide a framework for understanding

1.3 Simplify complex issues

1.4 Reduce areas of conflict

1.5 Encourage dialog in the event of disputes

1.6 Eliminate unrealistic expectations

Specifically it should embrace a wide range of issues. Amongst these are usually the following Services to be delivered Performance, Tracking and Reporting Problem Management Legal Compliance and Resolution of Disputes Customer Duties and Responsibilities Security IPR and Confidential Information Termination.

2.1. TYPICAL SERVICE LEVEL AGREEMENT CONTENTS

2.1.1. Definition of Services

SLA is an agreement that made between service provider and client. It is also called as service level contract. This is the most critical section of the Agreement as it describes the services and the manner in which those services are to be delivered. Standard services are different from customized services but this distinction is not critical. The information on the services must be accurate and contain detailed specifications of exactly what is being delivered.[3]

2.1.2. SLA parameters

SLA parameters are specified by metrics. Metrics define how service parameters can be measured and are typically functions. There are at least two major types of metrics. 1) Resource metrics are retrieved directly from the provider resources and are used as is without further processing. For example, transaction counts. 2) Composite metrics represents a combination of several resource metrics, calculated according to a specific algorithm. For example transactions per hour combine the raw resource metrics of transaction count and uptime. Composite metrics are required when the consumers need insightful and contextual information where raw numbers do not suffice. In [2], a third metrics referred to as a business metric has been defined. It relates SLA parameters to financial terms specific to a service customer.

2.1.3. Performance Management

A key part of a Service Level Agreement deals with monitoring and measuring service level performance. Essentially, every service must be capable of being measured and the results analysed and reported. The benchmarks, targets and metrics to be utilized must be specified in the agreement itself. The service performance level must be reviewed regularly by the two parties.[4]

2.1.4. Problem Management

The purpose of problem management is to minimize the adverse impact of incidents and problems. This usually specifies that there must be an adequate process to handle and resolve unplanned incidents and that there must also be preventative activity to reduce occurrence of unplanned incidents.

2.1.5. Customer Duties and Responsibilities

The important responsibility of the customer is to support the service delivery process. The SLA defines the relationship which of course is a two way entity. Typically, the customer must arrange for access, facilities and resources for the supplier's employees who need to work on-site.

2.1.6. Warranties and Remedies

This section of the SLA typically covers the following key topics Service quality Indemnities Third part claims Remedies for breaches Exclusions Force majeure.

2.1.7. Security

Security is a particularly critical feature of any SLA. The customer must provide controlled physical and logical access to its premises and information. Equally, the supplier must respect and comply with the Client's security policies and procedures.

2.1.8. Disaster Recovery and Business Continuity

Disaster recovery and business continuity can be of critical importance. This fact should be reflected within the SLA. The topic is disaster recovery is usually embraced within the security section. However, it is also frequently included within the Problem Management area. At the highest level, both these areas typically state that there must be adequate provision for disaster recovery and business continuity planning to protect the continuity of the services being delivered.

2.1.9. Termination

This section of the SLA agreement typically covers the following key topics:

- Termination at end of initial term
- Termination for convenience
- Termination for cause
- Payments on termination

3. PRESENT SLA'S

The Service Level Agreement (SLA) is incorporated into the Master Service Agreement and applicable to all services delivered directly to Customers of cloud service provider. The SLA is not applicable to unrelated third parties or third parties lacking privacy of contract with that particular cloud service provider. The uptime guarantees and the resulting SLA credits are applied in monthly terms unless specified otherwise. All SLA guarantees and information listed below:

SLA Credit Claim: To properly claim an SLA credit due, a customer user must open a Sales ticket by sending an email to Sales within seven days of the purported outage. Customer must include service type, IP Address, contact information, and full description of the service interruption including logs if applicable. SLA credits are issued as service credits on future billing cycles.

SLA Claim Fault: Customers making false or repetitive claims will incur a onetime charge of $50 per incident for such claims. False or repetitive claims are also a violation of the Terms of Service and may be subject to service suspension. Customers participating in malicious or aggressive internet activities thereby causing attacks or counterattacks do not qualify for SLA claims and shall be in violation of the Acceptable Use Policy.

Public Network: The cloud service provider (e.g., Server Intellect) guarantees 99.9% uptime on all public network services to Customers located their partner data centres. All public network services include redundant carrier grade internet backbone connections, advanced intrusion detection systems, denial of service mitigation, traffic analysis, and detailed bandwidth graphs.

Private Network: The cloud service provider guarantees 99.9% uptime on the service network services to Customers located in partner datacentres. All private network services include access to the secure VPN connection, unlimited bandwidth between servers, unlimited uploads/downloads to servers, access to contracted services, traffic analysis, and detailed bandwidth graphs.

Hybrid cloud: In a hybrid cloud environment, a *service level agreement*

(SLA) — a document between a service user and a service provider that defines uptime, availability, and performance — becomes more complicated than an SLA for a private cloud service, which is very similar if not identical to the SLA between a business unit and the IT organization. Given the current state of the world, what should a business do about managing service levels across cloud models? You should consider starting at

―home‖ and thinking about what's most important to the business. Thus, the SLA process begins by setting up a set of principles and requirements that are important to your organization's success in the market.

Redundant Infrastructure: The cloud service provider guarantees 99.9% uptime on the power and HVAC services to Customers located in our partner data centres. All computer equipment and related services are served by redundant UPS power units with backup onsite diesel generators. Specific guarantees with SLA information, Public Network, Private Network, and Infrastructure SLA listed below

Hardware Upgrades : The cloud service provider guarantees hardware upgrades will commence and complete within four hours of scheduled hardware upgrade maintenance windows. . Failure to install the hardware within the four hour time will result in a waiver of any one time installation fees. Hardware upgrades must be scheduled and confirmed in advance through the online ticketing system.

4. STANDARDIZE SLA'S

4.1. SLA has to discuss how the following security risks are handled

The past SLA's declares waivers if the promises are not met but do this really help the customer's in fulfilling their losses. The SLA's also have to discuss about how the security is maintained, what are the methods used in maintaining security and how customer complaints are taken care? The following are the security issues that SLA has to discuss [5]

4.1.1. Privileged user access.

Sensitive data processed outside the enterprise brings with it an inherent level of risk, because outsourced services bypass the "physical, logical and personnel controls" IT shops exert over in-house programs. Get as much information about the people who manage our data. Ask providers to supply specific information on the hiring and oversight of privileged administrators, and the controls over their access.

4.1.2. Regulatory compliance.

Customers are ultimately responsible for the security and integrity of their own data, even when it is held by a service provider. Traditional service providers are subjected to external audits and security certifications. Cloud computing providers who refuse to undergo this scrutiny are signalling that customers can only use them for the most trivial functions.

4.1.3. Data location.

When we use the cloud, we probably won't know exactly where our data is hosted. In fact, we might not even know what country it will be stored in. Ask providers if they will commit to storing and processing data in specific jurisdictions, and whether they will make a contractual commitment to obey local privacy requirements on behalf of their customers.

4.1.4. Data segregation.

Data in the cloud is typically in shared environment alongside data from other customers. In this Encryption is effective but isn't a cure-all.The providers should provide fact or evidence of that data would be in the encryption schemes were designed and tested by experienced specialists

4.1.5. Recovery.

The customer don't know where your data is stored ,a service providers should tell us what will happen to our data and service in case of a disaster. Any offering that does not replicate the data and application infrastructure across multiple sites is vulnerable to a total failure.[6]

4.1.6. Investigative support.

Investigating inappropriate or illegal activity may be impossible in cloud computing. Cloud services are especially difficult to investigate, because logging and data for multiple customers may be co-located and may also be spread across an ever-changing set of hosts and data centres. If we cannot get a contractual commitment to support specific forms of investigation, along with evidence that the vendor has already successfully supported such activities, then our safe assumption is that investigation and discovery requests will be impossible.[8]

4.1.7. Long-term viability.

Cloud computing provider will never go broke or get acquired and swallowed up by a larger company. But must be sure about the data will remain available even after such an event.

4.1.8. Future Work:

We see many avenues of future research in this area.One such avenue is based on scalability, which is considered an important aspect of cloud computing. Clouds however may not be able to scale indefinitely and when a resource limitation is encountered, a service provider may decide to delegate the tasks to other cloud providers, transparent to the consumer to avoid significant SLA violation penalties. Such a scenario creates research opportunities in SLA management. We anticipate investigating SLA aspects like accounting, monitoring of QoS parameters and condition violation in similar scenarios as future work. The current WSLA framework is based on XML and therefore limits the ability of matching in composition metrics to syntactical. Semantic Web tech-neologise can be used to enhance the descriptions and hence improve the quality of these matches. We believe that work done in [is relevant in this regard and can be extended to the cloud context.[7]

4.2.1. Security at Different Levels

We need security a following level erver accessecurity .Internet access security Database access security Data privacy security Program access security

5. CONCLUSION

The present SLA's discuss only about the services provided and the waivers given if the services not met the agreement, but this waivers don't really help the customers fulfilling their losses. We see a very legitimate need for a clear and formal methodology to handle SLAs in the context of cloud computing. WSLA, which suggests a very flexible architecture for managing SLAs between providers and consumers, seem to be the most suitable candidate. The waivers have to be made according to the type of business done by the customers. Besides the waivers the SLA has to discuss about many other issues like security policies, methods and their implementations. It also has to discuss what legal actions are taken if the services are misused by the customer.

6. REFERENCES

[1] Greg Boss, Padma Malladi, Denis Quan, Linda Legregni, Hall, ―Cloud Harold Computing‖,http://www.ibm.com /developerswork/websphere/zones
[2]. Service Level Agreement Definition and contents‖, http://www.service-level-agreement.net, accessed on March 10, 2009.
[3]. Service Level Agreement and Master Service Agreement‖, http://www.softlayer.com/sla.html,acces sed on April 05, 2009.
[4] .Server Intellect Service Level Agreement‖,http://www.serverintellect.c om/legal/sla.aspx, accessed on April 09, 2009.
[5]. http://www.cloudsecurity.org, accessed on April 10, 2009.
[6]. Sampling issues we are addressing‖, http://cloudsecurityalliance.org/issues.ht ml#15, accessed on April 09, 2009.
[7]. MikeKavis,‖Real time transactions in the cloud‖, http://www.kavistechnology .com/ blog/?p=789, accessed on April 12, 2009.
[8]. Secure group addresses cloud computing risks‖, http://www.secpoint .com/security-group-addresses cloud computing -risks.html, April 25, 2009.