Cloud Security Issues

Balachandra Reddy Kandukuri
bcrkkster@gmail.com

Ramakrishna Paturi V
ramu.paturi@gmail.com

Dr. Atanu Rakshit
arakshit@isquareit.ac.in

Advanced Software Technologies
International Institute of Information Technology
Pune, India

Abstract

In past three decades, the world of computation has changed from centralized (client-server not web-based) to distributed systems and now we are getting back to the virtual centralization (Cloud Computing). Location of data and processes makes the difference in the realm of computation. On one hand, an individual has full control on data and processes in his/her computer. On the other hand, we have the cloud computing wherein, the service and data maintenance is provided by some vendor which leaves the client/customer unaware of where the processes are running or where the data is stored. So, logically speaking, the client has no control over it. 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, Service Level Agreement (SLA), Software as a Service (SaaS), Cloud computing Security.

1. Introduction

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 explains 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:

- Identify and define the customer's needs
- Provide a framework for understanding
- Simplify complex issues
- Reduce areas of conflict
- Encourage dialog in the event of disputes
- 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.

978-0-7695-3811-2/09 $26.00 © 2009 IEEE
DOI 10.1109/SCC.2009.84

2.1. Typical Service Level Agreement Contents:

2.1.1. Definition of Services

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 often separated 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.

2.1.2. 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 analyzed 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.

2.1.3. 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.

2.1.4. Customer Duties and Responsibilities

It is important for the customer to understand that it also has responsibilities 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.

2.1.5. 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.

2.1.6. 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.

2.1.7. 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.

2.1.8. 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 privity 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 datacenters. 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 datacenters. 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.

Redundant Infrastructure: : The cloud service provider guarantees 99.9% uptime on the power and HVAC services to Customers located in our partner datacenters. 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:

Uptime Guarantee	SLA Credit
99.9%	Guaranteed
99.8%	5%
99.7%	10%
99.6%	15%
99.5%	20%
99.4%	25%
99.3%	30%
99.2%	35%
99.1%	40%
99.0%	45%
Less than 99.0%	50%

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

4. How to 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:

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 signaling 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 a shared environment alongside data from other customers. Encryption is effective but isn't a cure-all. The cloud provider should provide evidence that encryption schemes were designed and tested by experienced specialists.

4.1.5. Recovery.

Even if we don't know where your data is, a cloud provider 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.

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 centers. 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.

4.1.7. Long-term viability.

Ideally, 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.

4.2. Questionnaire's that SLA should answer

The SLA is the agreement document provider and customer. It has to answer the following questions:

- What are the resources provided to the customer? How resources will help to the customer? Are there any limitations to the number of resources?

- How the bills are generated? What are the payment modes? How the services are affected if the customer delays in paying bills? This should contain grace period and how the customer can get the services back after the payment when the services stopped?

-What happens if the SLA is not met? How data is handled when the service contract ends, the type of data returned to the company?

-What happens if the service contract withdrawn? How data will be handled and returned to the company?

- How the service uses event logs and who actually has access to the data on the backend?

-Who will check the security of cloud providers?

- Which of the SaaS employees has root and database access, and will anything prevent them from getting access to your corporate data? What controls are in place?

-Is the held data separated between clients or is it all stored on one huge database out there? How is data separated? How will the legal question of e-discovery be addressed should it arise as a business concern?

- In terms of service availability, can you get your vendor to sign a service-level agreement?

-What Security arrangements do you have in place with cloud service providers you rely on to deliver your service? What are you doing to build "trust in depth" in the cloud?

-Many of the key challenges on cloud computing arise at the border between your infrastructure and the cloud.

-How do you move resources from one side to the other? Is the cloud application dependant on storage that resides on your side of the border?

-What impact will that have on the bandwidth requirements? And how do you seamlessly move virtual machines between the cloud and your data center as demand grows and shrinks?

-These are all valid and interesting questions. But an even larger question looming like a dark cloud on the horizon is that of jurisdiction and legal status. Is stuff in the cloud on the same legal footing as stuff in your data center?

-How will the switch happen to public cloud when the private cloud infrastructure gets mixed out? Or would you be using the public cloud for just running your services?

-How secure is encryption Scheme

- How much safe is data from Natural disaster?
- Is it possible for all of my data to be fully encrypted?
- What algorithms are used? Who holds, maintains and issues the keys?

-How to ensure Users that both Data and Code are safe?

4.2.1. Security at Different Levels

We need security at following levels:

- Server access security
- Internet access security
- Database access security
- Data privacy security
- Program access Security

Questions

- What is Data Security at Physical Layer?
- What is Data Security at Network Layer?
- What about investigation Support?
- How much safe is data from Natural disaster?
- How much trusted is Encryption scheme of Service Provider**?**

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. 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, Harold Hall, "Cloud Computing", http://www.ibm.com/developerswork/websphere/zones/hipods/library.html, October 2007, pp. 4-4

[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, accessed on April 05, 2009.

[4]. "Server Intellect Service Level Agreement", http://www.serverintellect.com/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.html#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.