International Journal of Software Engineering and Its Applications
Vol. 10, No. 12 (2016), pp. 449-460
http://dx.doi.org/10.14257/ijseia.2016.10.12.37

Tenant - Vendor and Third-Party Agreements for the Cloud: Considerations for Security Provision

Lubna Luxmi Dhirani, Thomas Newe and Shahzad Nizamani

Department of Electronic & Computer Engineering, University of Limerick, Ireland
Department of Electronic & Computer Engineering, University of Limerick, Ireland
Dept. of Software Engineering,
Mehran University of Engineering & Technology, Pakistan
lubna.luxmi@ul.ie, thomas.newe@ul.ie, shahzad.nizamani@muet.edu.pk

Abstract

Cloud Computing has an expanding future in both business and Information Technology. With the expanding hybrid cloud model offering better services and convenience there are also a number of security problems associated with cloud standardization, multi-tenancy third party privity/sub-contracting, data-controller, outages, availability, monitoring and the service level agreements. This paper focuses on Hybrid Cloud Computing security in the context of a Tenant-Vendor-Third-Party environment and service level agreements. Limitations, opportunities and suggestions to mitigate the security risks are discussed and summarized.

***Keywords**: Cloud Computing; Security; Cloud Standards; Third-party privity; Data-controller; Outages; Availability; Monitoring; Service Level Agreements*

1. Introduction

Cloud Computing has revolutionized both IT and businesses by providing attractive benefits of reduced IT-related costs, resource availability, convenience and the pay-as-you-go model with customizations provided as an add-on [1][2].

Cloud computing offers many services including: Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS [3][4]) and four deployment models i.e. Public, Private, Community and Hybrid. Office 365 [5], Dropbox [6], Google App Engine [7] and Amazon Elastic Cloud Compute (EC2) [8] are few examples of the above mentioned services.

2.1. Cloud Models

Public clouds are formed by IT vendors who share their infrastructure, applications, platforms, storage, computing resources and processing power to other organizations considering them tenants. Public clouds are based off-premises and resources are shared among multiple tenants [1]. The tenants are liable to pay for the infrastructural resources consumed while the contract lasts.

Private Clouds are clouds formed within organizational premises and under their control [2]. The organization itself is responsible for the managing, monitoring and securing the infrastructure.

Community cloud involves sharing computing resources with other organizations having a shared goal [3].

The Hybrid cloud is formed when public and private clouds work together during high processing and cloud bursting situations [9]. What makes hybrid unique is: different

ISSN: 1738-9984 IJSEIA

deployment models are working collectively for a specific time-period, with the Quality of Service (QoS) and security being controlled by a mutually agreed Service Level Agreement (SLA) between the tenant and the vendor, thus promising a best-effort or guaranteed service [1].

Cloud vendors specialize in different areas for competitive advantages. Hadoop and MapReduce [3] dominate large scale computing where as the following vendors have created distinct competition in the open source cloud computing databases: Cassandra, MongoDB, CouchDB [10]. A vast range of platforms, application and services are designed for supporting cloud functionalities.

This paper focuses on various security challenges in a tenant-vendor-third-party environment. Section 2 discusses cloud standards, multi-tenancy, third-party privity, data controller, outages, availability and monitoring issues. Section 3 illustrates the SLAs, their mechanism, limitations and issues.

The authors have created scenarios in order to highlight the limitations and security challenges within the current tenant-vendor-third-party environment and a possible solution to the existing problems.

Summary and future work is presented in Sections 4 and 5.

2. Cloud Security Challenges

This section discusses security challenges introduced because of the tenant-vendor-third-party hybrid cloud arrangement.

2.1. Cloud Standards and Benchmarks

Lack of standardization and consistency is the foremost cause for cloud security breaches, since there is no mechanism to benchmark or audit the quality of service or evaluate the operational efficiency and reliability of the vendors. Few vendors have developed in-house models to create a systematic approach towards the hybrid cloud, but this approach could also lead to a tenant lock-in situation, as other vendors might be following different approaches or standards. In order to overcome this existing problem, various organizations *i.e.*, The National Institute of Standards and Technology (NIST) [9], International Organization for Standardization (ISO), International Electro technical Commission ISO/IEC 17788:2014 [11], Cloud Security Alliance (CSA) [12], Open Cloud Consortium (OCC) [3], *etc.* have developed some standards ensuring quality of service and authenticity which can been implemented by vendors. Though the above mentioned cloud standards need to be updated whenever a new functionality within the cloud environment is developed, designed or updated.

Harmony [13] and Serverbear [14] also provide a comparison on the types of services (Virtualization, Prices, Performance, UnixBench, I/O Benchmark, RAM, hard drive, Regional presence, Latency, *etc*) provided by a number of vendors. This can help tenants on deciding on the right vendor based on their resource, pricing and computational requirements.

The SMICloud Framework [15] also aids in comparing and ranking various Cloud Services with multiple attributes including Security and Privacy. The comparisons are made based on the Quality of Service provided by vendors. This Framework can be used if the tenant itself wishes to do a comparison but the drawback would be that the tenant would require accurate information from the vendors in order to perform a real evaluation.

Considering a multi-tenancy-vendor-third party subcontracting scenario, it is important for each of the third-party subcontractors to implement the same standards as those of the vendor to maintain trust between tenants-vendor-third party subcontractors.

2.2. Multi-tenancy

Multi-tenancy presents further security challenges related to authentication since multiple tenants are sharing the same infrastructure, resources and Internet Protocol (IP) Address on the cloud.

An example, threat can be if any one tenants database or applications have been affected by malicious activities, there is a chance that other tenants data or applications will be compromised also [16]. Amazon's Virtual Private Cloud (VPC) overcomes this limitation since it provides a networking layer called Elastic Cloud Compute (EC2) which logically isolates the tenants account from other users. With the VPC, the tenant also gains flexibility to create its own subnets, configure routing tables, network gateways and security settings [8]. The only limitation is that the platform only supports VPC for the Amazon clients from 2013 onwards.

Applications run and managed by tenants themselves in a multi-tenancy environment produces unnecessary traffic within the hybrid cloud, as a result of Virtual Machines (VMs) failing to identify the right path [17]. Considering a multi-tenancy-vendor-third party subcontracting scenario, it is a must for the vendors and sub-contractors to have a stable IaaS, because with increasing numbers of VM/Clones on a single IP, the tendency for server crashing problems and below par network performance increases as well. Especially when all VMs are being created, modified, or upgraded at more or less the same time this may lead to service disruption or an Outage. This disruption may be compared to a Denial of Service (DoS) problem and must be managed accordingly.

2.3. IT Third Party Privity

IT Third party privity means IT outsourcing. It is considered to be a security threat as well because outsourcing is being done by the vendor with or without the tenants consent, increasing the risks associated to privacy, data-controller, multi-tenancy, outages, availability, monitoring *etc.*

Providing cloud services in every country across the globe can lead to extremely low profit margins and higher maintenance costs, this leads to vendors sub-contracting their tenants based on regional location [18]. This type of vendor strategy exposes a tenant to various risks as mentioned before with a major threat being, what-if the third-party shuts down its operations? In practice minor tenants are the ones which are most affected [19][20]. Symantec Backup Executive Cloud [21] and Nebula [22] are two examples which give tenants a shutdown notice to allow them to download their business data and applications from the cloud. This solution is only practical for minor tenants however as the notice period given is short. Big tenants however still hold a strong position and will sue as per the service level agreements.

Amazon Web Services offers a huge range of third party products within its AWS environment [8] but in the case of any vulnerability reported from either the tenant or third-party side, AWS is responsible for sorting out the issue, however, the tenant's details are always kept confidential from the third-party which provides protection for a tenant. However in situations where the tenants do not have technical knowledge about the system functionality and data controller, vendors may skip port scans, vulnerability assessment and penetration testing [19] which are important jobs to be performed in a hybrid cloud environment. This may make the tenant susceptible to security risks [23].

2.4. Data Controller

This section discusses security aspects related to Data security, Governance, Risk and Control considering a multi-tenancy-vendor-third party subcontractor scenario in a hybrid cloud. Bearing this in mind, the risk of outsourcing the tenant's data and to maintaining data security is mitigated against by adhering to regulations for cloud vendors, such as:

1. In Europe vendors cannot export data out of the European Economic Area (EEA). Cloud providers holding Government information, are not allowed to move the information out of that particular country or state. Though a Government body can make the use of Model Form Agreements which are standardized contracts for exporting data outside EEA [20].

2. US-EU Safe Harbour laws have been progressive in securing the control of Data but again tenants need to make sure in which particular region their data is being processed, since some vendors might comply only with the local laws and not the international ones [16][24]. Trouble can ensue, if the region in which a tenant's data is being processed does not comply with the tenants host country's data protection laws.

3. As per Swiss and EU law special permissions are required while transferring data from one country to another based on if the recipient is covered by the Safe Harbour Regime and has a valid reason or requirement for acquiring or using that data [25].

4. Vendors are required to destroy tenant's information after the contract is over and provide a copy of the entire tenant backup to the tenant [26].

5. As per Swiss Data Protection Laws which are also in line with EU Law, if a tenant's data is being processed at a subcontractor's data centre [25], it is the Vendor's responsibility to act as a Data controller and make sure that the sub-contractor does not misuse, steal data or terminate operations without warning. It is also important for the vendor to monitor the Quality of Service (QoS) and conduct audits on the sub-contractors for authentication and security purposes.

6. The vendor should also make sure that the data is encrypted and controlled [19]. There should be an additional level of security to encrypt the data, so it is protected incase of any Distributed Denial-of-Service Attacks (DDoS) attacks or malicious attacks within the multi-tenancy environment [27][28].

7. EuroCloud is an initiative taken by various vendors within European countries. The core motive for it is to promote and stabilize the cloud computing environment in terms of innovation, quality and services; it is a two-tier approach between the vendor and the user [29].

8. Giant vendors like AWS do not guarantee Data Security in terms of modifying, adding, deleting, etc. and they clearly state that it is the user's responsibility to protect and create regular backups. All the vendors promise to provide is 99.95% service uptime or availability, which is in itself an obvious risk to tenant data [30].

9. In order to protect the data, it is important to transport it in encrypted format over the network and it should be decrypted at the required destination. This will protect the data even if it falls under unauthorized access [31] such as: Metadata Spoofing Attack [32], Wrapping attack [33], Cross site scripting or Distributed Denial-of-Service Attacks, SQL Injection Attacks, Malware Injection Attack [28][34], *etc*. In addition to encryption, firewalls needs to be installed on the network to further protect against the above mentioned attacks [27].

10. There are tools like Vormetic, which can be directly implemented within Amazons Elastic Cloud Compute, IBM Smart Cloud, Rackspace, *etc*. without re-architecting their applications for data encryption and strong Key management but that is an add-on expense for the tenant to invest in [35] as giant vendors like AWS do not otherwise guarantee or provide encryption services [8].

Amazon Inspector, is a new data controller monitoring tool provided by AWS which analyzes the tenants instances and generates a report if any security or compliance issue is found [36]. It is a kind of watchman system which informs you of any vulnerable or weird activity but the liability to fix any detected issue rests with the tenant.

The biggest challenge for the giant vendors is the General Data Protection Regulation (GDPR) which is the new data protection framework to be implemented across Europe and will replace the Safe Harbour by 2018. It will cover 50 different components and it is expected to better comply with the latest cloud standards. In the next two years, all of the vendors working in the EU region will have to follow the GDPR and for that it will be necessary for them to start modifying their systems to best fit into the new framework [37]. Vendors which fail to do so will have to pay a penalty of 4% of their annual global turnover.

The majority of the risks outlined here can be mitigated and controlled with a strong service level agreement, though there is no such tool through which a tenant can actually monitor the promised level of QoS being provided by the third-party. This is only visible between the vendor and Subcontractor. Vendors and subcontractors share mutual benefits, the vendor's sub-contract services to expand their reach across the globe, where as for these small subcontractors it is hard to compete in an aggressive market with better offerings, so they settle down with regular outsourced contracts.

2.5. Outages, Availability and Monitoring

In the context of IaaS, it is very important to identify the security measures a vendor is committed to under a disaster recovery and Outage situation [38]. Irrespective of the Cloud boom, the maximum uptime service by all giant vendors is 99.95% (best effort), which means 4 hours and 23 minutes of Outage per year, downtime or unavailability for various reasons (*i.e.,* Upgrades, natural disaster, network issues, bandwidth, security issue, *etc.)* [39]. Giant vendors utilize high-end monitoring tools which are designed to generate an alert before a node fails, creating ample time to replace it rather than going through an Outage. AWS uses tools like Elastic Load Balancer, Auto-Scaling, and Cloud Watch to balance the loads on multiple VMs. When the load increases or decreases, the cloud smartly scales-up or down as per the tenants processing load and CloudWatch can work in conjunction with Elastic Load Balancer and Auto-Scaling [8] to monitor the overall VM performances [40]. Despite these smart tools AWS fails to enhance its guaranteed service uptime.

The best efforts service uptime and availability clearly draw attention to the facts of cloud services being subcontracted to third parties, otherwise there is no point for giant vendors to stick to 99.95% "best efforts uptime and not guaranteed uptime". This space is maintained by the vendors to cover up the faults or risks that arise as a result of subcontracting.

Many researchers have come up with diverse concepts of InterCloud Co-coordinators, brokers [1] [40], Requirements Engineering and Risk Management for monitoring [41] and mitigating the risks associated with the cloud but none of the giant vendors have adopted these suggestions as that would minimize the financial profits and flexibilities they benefit from.

As shown in Figure 1, an IaaS physical layer comprises of four basic components: Network, Physical Management, Host and Virtualization [42]. In short, tenants rent the IaaS of a vendor and if the tenant has some extra requirements, there are tools available for supporting tenants to buy on a monthly or usage basis for supporting its applications.

Consider a multi-tenancy-vendor-third party subcontracting scanerio where there is no system for tenants to track or control the number of applications being processed on a third-party's facility. The tenant's console only provides views to its connection with the vendor, which means an outage or unavailability can arise anytime without any prior warning or notice as there is no monitoring system between the tenant and subcontractor.

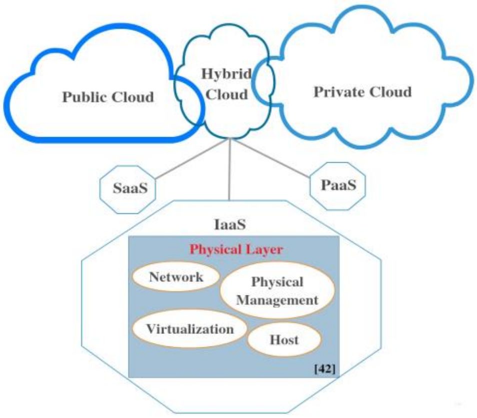

Figure 1. Components of IaaS Physical Layer

3. Service Level Agreement

A Service Level Agreement (SLA) is a mutually agreement document between the tenant and vendor. It comprises the terms and conditions of the services provided by the Vendor which covers all aspects related to Service Descriptions, Performance Metrics, Benchmarks, Continuity or Outages, Security and Risk Management, *etc*. It is a contract which gives rights to the tenant for claiming service credits if the Vendor fails to meet the guaranteed service uptime or other promised criteria [43]. Despite having such a document, there are still a lot of loopholes and at times small tenants are often ignored. For Example: Vendors might just mention Service uptime as 99.95% best efforts, but is that per month or per year? Tenants need to be aware before signing the contract as later they might end up getting absolutely no Credit claims. Every vendor has its own criteria; few accept the service credit to be used right away and few accept the credit note to be used for future payments, there is also a time limit of 30 days for contacting the vendor over a SLA violation, so the tenant might miss the opportunity for claiming the credit [44].

The promised services and prices may also vary between tenant-vendor and vendor-subcontractor as shown in Figure 2

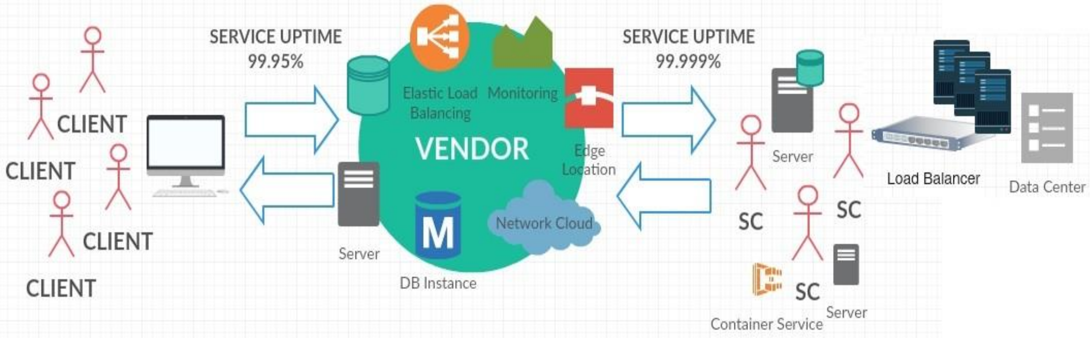

Figure 2. Multi-tenancy Environment: A giant Vendor Sub-contracting Services to a Third-party in a Multi-tenant Environment

To facilitate situations where on the spot requests are made a response from seconds to milliseconds is required. For example: Amazon’s latency in its cloud offerings and services is around 50 milliseconds [45].

All conversations for extra services requested or granted are communicated in a Web Service Level Agreement Language and Framework (WSLA) [46] between the tenant and the vendor, which also performs SLA negotiations (*i.e.*, time, price, reliability) and monitoring the requirement to be met [47]. Various research projects for SLA

Management (*i.e.*, mOSAIC [48], ETICS [49] *etc.*) have been done before but none have been adapted by the vendors yet.

3.1. SLA Metrics

SLA Metrics are measures for evaluating the performance levels of SLAs based on: CPU capacity, VM memory size and boot time, storage size, scalability, auto scaling, load balancing, availability, response time, and maximum number of VMs configured on a single server [50].

In order to make the concept clear, a multi-tenant-vendor-third party subcontractor example has been given in Figure 3. Tenants A, B, and C are using a vendors public cloud services during peak performance hours and all three tenants vary in respect of operation, computation, resources optimization and demands.

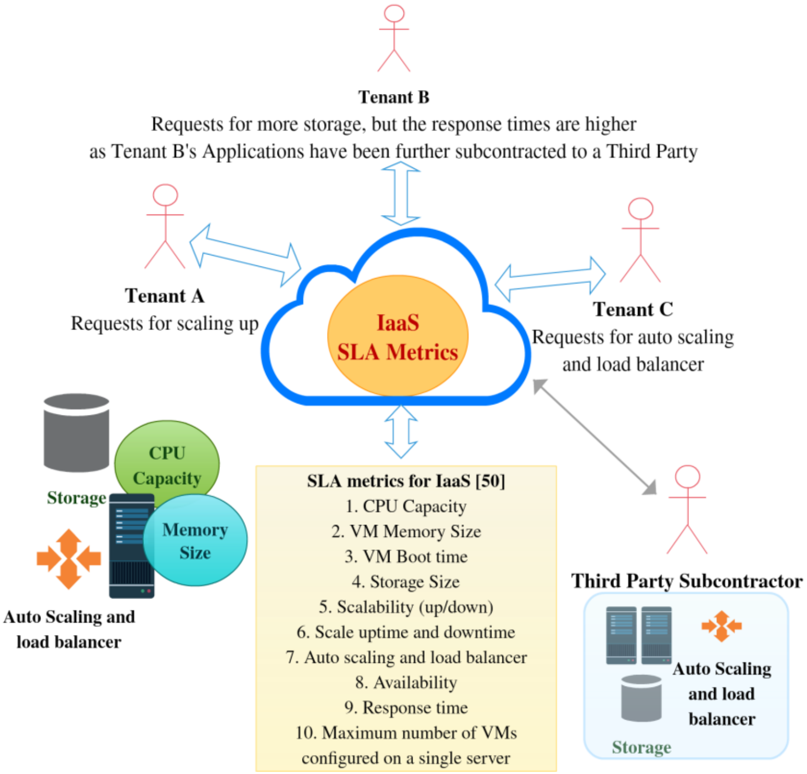
Tenant B
Requests for more storage, but the response times are higher
as Tenant B's Applications have been further subcontracted to a Third Party
Tenant A
Requests for scaling up
IaaS
SLA Metrics
Tenant C
Requests for auto scaling
and load balancer
Storage
CPU Capacity
Memory Size
Auto Scaling and load balancer
SLA metrics for IaaS [50]
1. CPU Capacity
2. VM Memory Size
3. VM Boot time
4. Storage Size
5. Scalability (up/down)
6. Scale uptime and downtime
7. Auto scaling and load balancer
8. Availability
9. Response time
10. Maximum number of VMs configured on a single server
Third Party Subcontractor
Auto Scaling and load balancer
Storage

Figure 3. Multi-tenancy Environment: Giant Vendor Subcontracting Services for its Different Tenants based on their Requirements, Location, Resources and Demands

Tenant A (a software house) requests more VMs where as Tenant C (a retailer) requests for auto scaling and load balancer so the requirement for VMs might vary on an hourly basis. The vendor first checks the availability of free VMs in its public cloud, the tenants SLA/contract and sends back a WSLA comprising of the pricing for on spot, reserved or on-demand services requested. If the tenants A and C approve, they will get the services immediately or at times there is a space for negotiation.

Tenant B (an online storage website) has sent a request demanding for more storage but the requests waiting time has crossed the conventional 50-100 ms response time. This puts Tenant B in a uncertain state, since its operational efficiency is being affected due to storage limitations. Since the vendor has subcontracted Tenants B services to a third party, the requests for any demand go to the vendor and then further forwarded to the subcontractor. Keeping this in mind, the response time for any requests or responses will be double (*i.e.*, 50-100 ms x 2).

In such a situation, it is crucial for giant vendors to either have more than one sub-contractor or itself have enough resources to grant its tenants request. None of the tenants will take a denial of resources which can lead to a DoS for which they are ready to pay further. Either requests for services made are accepted or rejected, the communication between Tenant B, vendor and subcontractor takes place in the form of exchanging WSLAs.

3.2. SLA Framework

Two standards called: Web Service Agreement (WS-Agreement) and WSLA Language and Framework are widely implemented for describing SLAs in a Service Oriented Architecture [46][50]. The WSLA framework comprises of SLAs in an Extensible Markup Language (XML) [51] document which participates (*i.e.*, publish, negotiate, commitment, provision, monitor, management reporting, terminate) during the entire contract lifecycle [47].

Figure 4 depicts an entire SLA lifecycle for tenants A, B and C.

Initially all tenants and vendors publish their SLAs and exchange them. The vendor and tenants check the requirements that match and enter for negotiating on the requirements which differ. The negotiation phase comprises flexibility, where the tenants and vendors can bargain on the pricing, duration, resources, *etc.* being offered or provided. Post negotiation, if both parties agree on a standard SLA, a digital signature is placed as a commitment and confirmation of the contract. Later provisioning or deployment involves implementing the service which is evaluated on a regular basis and monitored within the WSLA Framework. If at any stage the services are violated or not met, an alert is generated to the management to either enter into the negotiation phase again and if the negotiation fails it leads to terminating the contract.

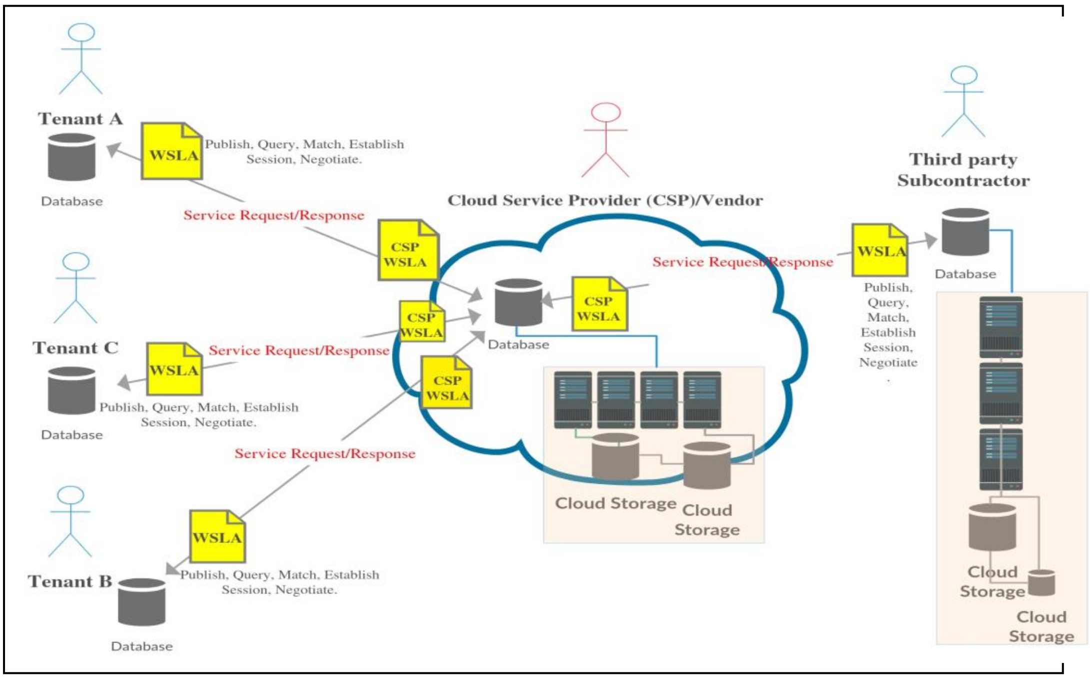
Tenant A
WSLA
Publish, Query, Match, Establish Session, Negotiate.
Database
Service Request/Response
CSP WSLA
Cloud Service Provider (CSP)/Vendor
Third party Subcontractor
WSLA
Database
Service Request/Response
Publish, Query, Match, Establish Session, Negotiate
CSP WSLA
CSP WSLA
Database
Tenant C
WSLA
Service Request/Response
CSP WSLA
Publish, Query, Match, Establish Session, Negotiate.
Database
Service Request/Response
Cloud Storage
Cloud Storage
WSLA
Tenant B
Publish, Query, Match, Establish Session, Negotiate.
Database
Cloud Storage
Cloud Storage

Figure 4. Multi-tenancy Environment: SLA Negotiation between Tenants, Vendor and the Third Party Subcontractor

At each stage of the phases mentioned above, the SLAs are monitored and measured but this particular scenario is between a tenant and a vendor and subcontracting will not help since the giant vendors do not put the tenants in direct contact with the subcontractors. This can lead to data security risks as mentioned previously.

4. Summary

Undoubtedly, cloud computing has taken technology, business and applications to the next level of technological innovation. The obstacles it faces are security, transparency of services and lack of standardization in a three tier model (Tenant-Vendor-Third-Party Subcontractor). It is proposed that vendors implement a uniform cloud standard on their entire operational three tier model to overcome the limitations of vendor-lock in. Regular audits with respect to the standards will validate vendors on their QoS and validate on multi-tenancy, data controller, risk and governance issues as well. Some laws and data protection techniques have been cited to prevent data integrity, privacy, confidentiality and availability breaches. It is also recommended that vendors provide a minimum time (*i.e.,* not more than 100 ms) to respond to tenant resource requests in terms of subcontracting to avoid outages and VMs crashes. Cloud adaption and further outsourcing of IT services can only be accepted by tenants if a transparent method is provided where due control is given. Otherwise such a model can leave many potential security problems for the tenant.

5. Future Work

We are currently working on designing a framework and utility for monitoring and tracking the SLAs in a tenant-vendor and third party subcontractor situation. This will provide authentication services and transparency of service by vendors to tenants.

References

[1] R. Buyya, C. Shin Yeo, S. Venugopal, J. Broberg and I. Brandic, “Cloud Computing and emerging It Platforms: Vision, Hype, and reality for delivering computing as the 5th Utility”, Future Generation Computer Systems, Elsevier, vol. 25, **(2009)**, pp. 599-616.

[2] R. Buyya, J. Broberg and A. Goscinski, “Cloud Computing Principles and Paradigms”, John Wiley & Sons, Inc **(2011)**.

[3] J. Rhoton, Cloud Computing Explained, Recursive Press, Second Edition, **(2011)**.

[4] C. Rong, S. T. Nguyen and M. G. Jaatun, “Beyond lightning: A survey on security challenges in cloud computing”, Computers and Electrical Engineering, Elsevier, vol. 39, **(2013)**, pp. 47–54.

[5] https://products.office.com/en-IE/ [Accessed 20 August 2015]

[6] https://www.dropbox.com/ [Accessed 2 February 2016]

[7] https://cloud.google.com/ [Accessed 2 February 2016]

[8] https://aws.amazon.com/ec2/ [Accessed 10 January 2016]

[9] http://selil.com/CLOUD/thoughtData/1/NIST_CCSRWG_092_NIST_SP_500-291_Jul5.pdf [Accessed 20 February 2016]

[10] J. Han, Haihong E., G. Le and J. Du, “Survey on NoSQL Database”, IEEE – 2011 6th International Conference on Pervasive Computing and Applications (ICPCA), **(2011)**.

[11] https://www.iso.org/obp/ui/#iso:std:iso-iec:17788:ed-1:v1:en [Accessed 23 February 2016]

[12] https://cloudsecurityalliance.org/ [Accessed 23 February 2016]

[13] https://cloudharmony.com/ [Accessed 22 September 2015]

[14] http://serverbear.com/ [Accessed 4 January 2016]

[15] S. K. Garg, S. Versteeg and R. Buyya, “SMICloud: A Framework for comparing and Ranking Cloud Services”, Fourth IEEE International Conference on Utility and Cloud Computing, **(2011)**.

[16] D. Zissis and D. Lekkas, “Addressing Cloud Computing Security Issues”, Future Generation Computer Systems, Elsevier, vol. 28, **(2012)**, pp. 583-592.

[17] H. Ballani, K. Jang, T. Karagiannis, C. Kim, D. Gunawardena and G. O’Shea, “Chatty Tenants and the Cloud Network Sharing Problem”, 10th USENIX Symposium on Networked Systems Design and Implementation, **(2013)**.

[18] T. J. Trapplee, “When there is a third party in the cloud”, ComputerWorld, **(2012)** July 30.

http://www.computerworld.com/article/2505135/cloud-computing/when-there-s-a-third-party-in-the-cloud.html [Accessed 15 October 2015]

[19] Cloud SLA Considerations for the Government Consumer. MITRE (**2015)** http://www.mitre.org/sites/default/files/pdf/cloud_sla_considerations_government.pdf [Accessed 1st December 2015]

[20] P. Nolan and O. Tobin, "Cloud Computing in the public sector: risks and reward", Public Affairs Ireland January/February **(2011)**

[21] http://www.pcworld.com/article/2067360/symantec-to-shut-down-backup-execcloud.html [Accessed 30 November 2015]

[22] https://www.nebula.com/ [Accessed 30 November 2015]

[23] European Network and Information Security Agency, Cloud Computing–Benefits, Risks, and Recommendations for Information Security, http://www.enisa.europa.eu/act/rm/files/ deliverables/cloud-computing-risk-assessment/ at_download/fullReport, **(2009)**.

[24] S. Marston, Z. Li, S. Bandyopadhyay, J. Zhang and A. Ghalasi, "Cloud Computing – The Business Perspective", Elsevier, Decision Support Systems, vol. 51, **(2011)**, pp. 176-189.

[25] DR Ursula Widmer, "Cloud Computing and Data Protection", Who'swholegal, **(2009)** July http://whoswholegal.com/news/features/article/18246/cloud-computing-data-protection/ [Accessed 10 January 2016]

[26] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing", Elsevier. Journal of Network and Computer Applications, vol. 34, **(2011)**, pp. 1-11.

[27] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Kpnwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica and M. Zaharia, "A View of Cloud Computing", Communications of the ACM, vol. 4, no. 53, **(2010)**.

[28] S. VivinSandar and S. Shenai, "Economic Denial of Sustainability (EDoS) in Cloud Services using HTTP and XML based DDoS Attacks", International Journal of Computer Applications (0975-8887), vol. 41, no. 21, (**2012)** March.

[29] http://www.cloud28plus.eu/content/What-is-EuroCloud-Europe-- [Accessed 16 February 2016]

[30] S. Zardari, "Trouble in the cloud leaves behind businesses tied to their servers", The Conversation, **(2014)** May 15.

[31] M. Mowbray, "The Fog over the Grimpen Mire: Cloud Computing and the Law", Scripted Journal of Law, Technology and Society, vol. 6, no. 1, **(2009)** April.

[32] Meiko Jensen J ̈orgSchwenk, Nils Gruschka, Luigi Lo Iacono, "On Technical Security Issues in Cloud Computing", IEEE International Conference on Cloud Computing **(2009)**.

[33] Nils Gruschka and Luigi Lo Iacono, "Vulnerable Cloud: SOAP Message Security Validation Revisited", IEEE International Conference on Web Services **(2009)**.

[34] Y. Sun, J. Zhang, Y. Xiong and G. Zhu, "Data Security and Privacy in Cloud Computing. International Journal of Distributed Sensor Networks", 190903, **(2014)**, p. 9.

[35] http://www.vormetric.com/sites/default/files/wp-data-security-in-the-cloud.pdf [Accessed 6 December 2015]

[36] R. Miller, "Amazon Inspector Finds Security Issues For You", http://techcrunch.com/2015/10/07/amazon-inspector-finds-security-issues-for-you/ October 7, 2015 [Accessed 12 January 2016]

[37] http://itknowledgeexchange.techtarget.com/it-compliance/rsa-2016-adobe-google-microsoft-prepare-eu-gdpr/ [Accessed 10 March 2016]

[38] "Disaster Recovery and Business Continuity," The SLA Zone, http://www. sla-zone.co.uk/disaster.htm [Accessed June 29, 2010]

[39] B. R. Kandukuri, R. Paturi V. and Dr. A. Rakshit, "Cloud Security Issues", IEEE International Conference on Services Computing, **(2009)**.

[40] R. Buyya, R. Ranjan and R. N. Calheiros, "InterCloud: Utility-Oriented Federation of Cloud Computing Environments for Scaling of Application Services", C.-H. Hsu et al. (Eds): ICA3PP 2010: Part I, LNCS 6081, Springer-Verlag Berlin Heidelberg 2010, **(2010)**, pp. 13-31.

[41] S. Zardari and R. Bahsoon, "Cloud Adaoption: A Goal-Oriented Requirements Engineering Approach", SECLOUD 2011. ACM 978-1-4503-0582/11/05.

[42] Adapted from: O. Sharma, P. Das and R. K. Chawda, "Hybrid Cloud Computing with Security Aspect", International Journal Innovation, Adv. Computer Science, vol. 4, no. 1, **(2015)**, pp. 76-80.

[43] http://www.informationweek.com/cloud/infrastructure-as-a-service/cloud-slas-improvements-still-needed/a/d-id/1318730 [Accessed 20 August 2015]

[44] S. A. Baset, "Cloud SLAs: Present and Future", ACM. dl.acm.org/ft_gateway.cfm?id=2331586 [Accessed 10 August 2015]

[45] A. Hickey, **(2010)** March 19, "Cloud SLAs Add New Level of 'Confidence'", ChannelWeb, http://www.crn.com/news/applications-os/224000198/cloud-slas-add-new-level-of-confidence.htm [Accessed 20 November 2015]

[46] A. Keller and H. Ludwig, "The WSLA Framework: Specifying and monitoring service level agreements for web services", Journal of Network and Systems management, vol. 11, no. 1, **(2003)**, pp. 57-81.

[47] K. Bernsmed, M. G. Jaatun, P. H. Meland and A. Undheim, "Security SLAs for Federated Cloud Services", Sixth International Conference on Availability, Reliability and Security. IEEE, **(2001)**.

[48] S. Venticinque, R. Aversa, B. Di Martino, M. Rak and D. Petcu, "A Cloud Agency for SLA Negotiation and Management", M. R. Guarracino, (Eds.): Euro-Par 2010 Workshops, LNCS 6586, Springer-Verlag Berlin Heidelberg **2011**, **(2011)**, pp. 587-594.

[49] ETICS (Economics and Technologies for Inter-Carrier Services), 2011. https://www.ict-etics.eu/ [Accessed 16 February 2016]

[50] M. Alhamad, T. Dillon and E. Chang, "Conceptual SLA Framework for Cloud Computing", 4th IEEE International Conference on Digital Ecosystems and Technologies, **(2010)**.

[51] A. Andrieux, K. Czajkowski, A. Dan, K. Keahey, H. Ludwig, J. Pruyne, J. Rofrano, S. Tuecke and M. Xu, "Web services agreement specification (WS-Agreement)", In: Global Grid Form, **(2004)**.

Authors

Lubna Luxmi Dhirani, PhD student in the Department of ECE at the University of Limerick. PhD research project is based on designing a System for Securing the Hybrid Cloud in a tenant-vendor-third party situation. She has done MSc in Business Information Technology (2008) and B.Eng in Computer System Engineering (2006). Lubna has worked as a lecturer for 3 years and taught various IT-based courses at SZABIST – United Arab Emirates Campus and ISRA University, Pakistan. She did her Bachelors in Computer Systems Engineering from Mehran University of Engineering & Technology, Pakistan.

Thomas Newe, Senior Lecturer in Computer Engineering in the Department of Electronic & Computer Engineering at The University of Limerick. He holds a B.Eng. in Computer Engineering (1991), a Masters in Engineering in Security Protocol Design (1996) and a PhD in Formal Logics for Security Protocol Verification (2003).He has been a University of Limerick faculty member since 1994. His research interest include: Wireless Sensor Systems and Networks, Security protocol design for Data and the Cloud, Network Security, Security protocol formal verification methods, Cryptography/Encryption algorithms, Embedded system programming, Digital design, Programming languages, Operating systems, Smart cards security protocols, Digital Watermarking and Watermark Benchmarking tools. He has graduated a number of PhD students in the broad area of network security. His students are funded from a variety of sources including: EU, SFI, IRCSET, Internationally and industrially funded.

Shahzad Nizamani, Assistant Professor in the Department of Software Engineering at Mehran University of Engineering & Technology. He did his Bachelors in Software Engineering (2004) and Masters in Information Technology (2006) and PhD in Cloud Computing (2012). His research interests are: Services Oriented Architectures in Cloud Computing, Knowledge Management, Programming Languages, Semantic Technologies and Mobile Computing.