



SLA assurance in cloud computing: a trust issue

S.B. Dash, H. Saini, T.C Panda and A. Mishra

Orissa Engineering College, Orissa, India.

ARTICLE INFO

Article history:

Received: 26 March 2014;

Received in revised form:

20 July 2014;

Accepted: 29 July 2014;

Keywords

Service Level Agreement(SLA),

Cloud computing models,

Cloud service providers.

ABSTRACT

Most of the organizations are running their applications in cloud due to reliability, scalability, high performance, low band width and trust on cloud service provider(CSP). The cloud service providers provide the services to the registered cloud users on payment basic across the globe. The cloud services are basically categorized as SaaS, PaaS, and IaaS . The services are available to the users depending on cloud deployment and the SLA(service level agreements) between the service providers and the users. SLAs gives a transparent view to the cloud users which includes the delivery ability of a service provider, the performance target of the user's requirement, the scope of guaranteed availability of the cloud services The main objective of this paper is to provide a clear idea about the cloud service level agreements and the cloud computing models.

© 2014 Elixir All rights reserved.

Introduction

Cloud computing is a next generation computing platform that helps the users to share the resources through communication mediums. According to National Institute of Standards and Technology (NIST) one of the most accepted definition of cloud computing is "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction".[1] European Community for Software and Software Services (ECSS) defines "cloud computing as the delivery of computational resources from a location other than your current one".[1,2,3] So cloud computing is a distributed computing environment that provides a virtualized environment to the cloud users for accessing and exchanging their applications and data through internet.[4,5] The figure-1 shown below gives a clear idea regarding the infrastructure requirements for cloud deployment.

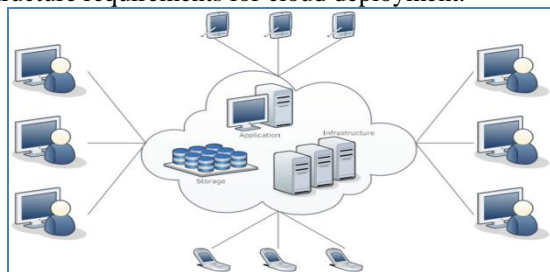


Figure-1 (infrastructure requirements for cloud deployment)

The key advantages of cloud computing

Broad Network Access.

The cloud services are provided to the requested users through web based applications. The users will access these services by using various heterogeneous platforms like desktop computers, laptops, mobiles from anywhere across the globe.

Scalability Of Infrastructure.

Changing in physical infrastructure i.e adding of new cloud nodes and deleting the nodes can be easily managed by the cloud service providers. So to use these infrastructure by the cloud users is simple and can be scaled according to the users requirements.[6]

Flexibility/Elasticity:

Users can access computing resources as and when needed, without the knowledge of technical infrastructure and human interaction. The capabilities will be managed by the service providers.

Unlimited Storage space.

Due to advancement in cloud data center architecture and virtualization technique all most unlimited storage will be provided to the registered users. So the cloud users will not have to be worried about the limited storage spaces.

Easy Access to Information.

Once registered in the cloud environment any one can access the information from any location provided, there is an Internet connection.

Location Independence.

Cloud interfaces are location independent and they can be accessed by well established interfaces such as Web services and Web browsers, so that no knowledge about exact location of the user is required. It gives a high level of abstraction to the user's data.

Economy And Cost Effectiveness.

The economy and cost effectiveness of the cloud environment depends upon the uses of service models and the deployment models. No physical infrastructures and software are required to run the user's applications. Everything will be provided by the service providers. So if larger numbers of cloud deployment models are implemented, then that will be advantageous for service providers as well as the cloud users. The users will use the services on subscription basis.[6,7]

Reliability

Due to the high reliability and trust worthiness most of the organizations are using cloud to deploy their applications and data. Use of multiple access is one of the advantages of cloud computing.

Sustainability

Cloud computing platform provides an efficient source utilization mechanism that makes the cloud environment sustainable and more popular among the cloud users.

Backup and Recovery.

All the user's applications and data are stored in cloud data centers. Providing security to the user's data is the responsibilities of the service providers. The backup and the recovery mechanism are handled to recover the information and the data. The replication and migration techniques are used for virtualization of data centers.[6]

Cloud service level agreements(SLA)

A Service Level Agreement (SLA) is a contract document or a formal negotiated agreement based upon the purpose and objectives that exists between the Cloud Service Providers and the cloud users. It includes the brief terms and conditions upon which the services being provided by the service providers. SLAs gives a transparent view to the cloud users for understanding about the cloud environment, which includes the advantages and disadvantages of the cloud, cloud services, cloud deployment and security issues ,responsibilities, guarantees and warranties of the services. [8,9,10,11] The figure-2 shown below gives clear idea about the SLA.

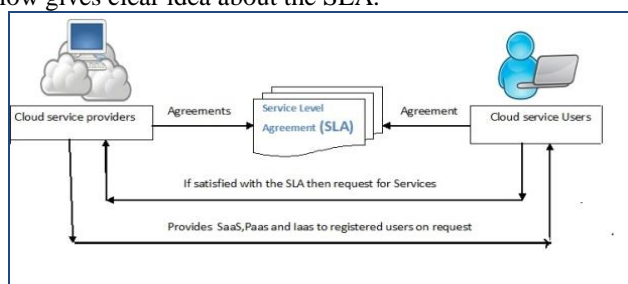


Figure-2(The cloud SLA.)

Needs of using SLA

- It gives a clear idea about the cloud service providers.
- It describes the list of services (SaaS, PaaS and IaaS) the providers will provide along with complete description of each service.
- The purpose and objectives about the business level policies i.e Service Level Agreement (SLA) in transparent manner, which includes the roles of the cloud service providers and the cloud users.
- It is used to know about the key security and privacy management policies for cloud environment.
- It monitors the service quality, performance, priorities, and responsibilities from service point of view.
- It gives a transparent view to Know about the service management requirements in case of cloud service failure.

Types Of SLA

Service Level Agreement (SLA) is important for using the cloud services, as it is a contract for business arrangements of all types, that understood by both service providers and the users. So based on the types of users and the services , SLAs are classified into 5 types.[8,11]

Customer-based SLA: It is the agreement with entity personal group which covers all services use by the users.

Service-based SLA: It is a contract or agreement between the cloud service provider and all registered users using the service.

Multilevel SLA: Such SLA consist of different levels, each level shows the situations of different customers for same service.

Customer level SLA: It contains all SLA (Service Level Management) issues relevant to group of particular users.

Service level SLA: It contains all SLA (Service Level Management) issues relevant to specific service, in relation with user group.

Components Of SLA

An SLA defines the delivery ability of a provider, the performance target of the user's requirement, the scope of guaranteed availability of the services. A list of SLA component descriptions are included below[9,10,13,14,15,16]

Business level objectives:

An organization must define *why* it will use the cloud services before it can define exactly what services it will use. This part is more organizational politics than technical issues: Some groups may get funding cuts or lose control of their infrastructure.

Responsibilities of both parties:

It is important to define the balance of responsibilities between the Cloud service provider and the cloud user. For example, the provider will be responsible for the Software-as-a-Service aspects, but the users may be mostly responsible for his VM that contains licensed software and works with sensitive data.

Cloud Security

This includes organizational and technical issues related to keeping cloud services at an acceptable level of security by ensuring the computing resources available and usable by its authentic users. Security threats to cloud infrastructure would affect multiple users even if only one site is attacked. These risks can be overcome by using encrypted file systems, security applications, data loss software and buying security hardware.

Privacy in Cloud.

Privacy is the process of making sure that the user's data remains private, confidential and restricted from unauthorized users. Due to data virtualization the users data may be stored in various virtual data centers rather than in the local computers. So the unauthorized users may access the private information of the authorized users. Data authentication is one of the most popular options of security before putting the sensitive data into cloud.

Data integrity and Reliability

Using cloud computing anyone from any location can access the data. Cloud does not differentiate between common data and sensitive data. So an important aspect of cloud services is availability of user's data with reliability. It is necessary for the cloud service provider to ensure the integrity by making their system capable to check over the cloud data from any unauthorized access.

Performance and Bandwidth cost.

The major issues that can affect performance in cloud based environment is due to the unethical transaction-oriented and data access applications. So the users who are at a long distance from cloud providers may experience high latency and delay, this is due to the availability bandwidth in the network. Bandwidth cost may be low for smaller Internet-based applications, which are not data intensive, but could significantly, grow for data-intensive applications. The service providers instead of saving money on hardware, they should spend more for the bandwidth. This can deliver intensive and complex application over the network.

Business continuity/disaster recovery.

The users should ensure ,the provider maintains adequate disaster protection. Two examples come to mind: Storing valuable data on the cloud as backup and cloud bursting (switchover when in-house data centers are unable to handle processing loads).

Table-1: Types of Cloud services

SERVICES	ADVANTAGES
<p>Infrastructure as a Service (IaaS) is one of the three fundamental service models of cloud computing . In this model the users are allocated with computing resources in order to run their applications. The computing services are provided in a virtualized environment i.e in cloud by using a communication network. The best known example of IaaS is Amazon Cloud Formation, Amazon EC2. It can be implemented by utilizing the concepts like Enterprise infrastructure, Cloud hosting, and Virtual Data Centers (VDC). Network as a service (NaaS) is a category of cloud infrastructure services where the user can use the network connectivity as a services. NaaS involves the optimization of resource allocations and resource computing in the network. VPN, and bandwidth on demand are the common example of NaaS[20,21,22,23]</p>	<ol style="list-style-type: none"> 1. Resources are available on demand as and when the user requires it. That means the user will not have to worry about the Infrastructure required to run the application. so this scalable. 2. In IaaS the Infrastructure i.e the virtualized environment is set up and maintained by the cloud provider. So no investment in hardware for the users. As it saves the implementation cost and time of execution. 3. The service can be accessed on demand and the client only pays for the resource or application used not for the Infrastructure 4. The service can be accessed from any location 24X7 provided there is an internet connection. So IaaS is location independent. 5. Physical security of user's data is the responsibility of the cloud provider. So the time required to give security to data is saved. 6. The chance of system failure is less. Any case of failure will be smoothly handled by the service provider. So it is fault tolerant.
<p>Platform as a Service(PaaS) is a category of cloud computing service model that provides the developers a platform to build and use applications and services by using a communication network. PaaS services are available in the cloud and accessed by users by using web browsers. In this model, cloud service providers provides a platform which includes operating system, programming language execution environment, database, and web server. The users can use these services to develop and deploy their own applications. AWS Elastic Beanstalk, Cloud Foundry, Heroku, Force.com, OrangeScape are some examples of well known PaaS providers . In PaaS services the user has to pay for a subscription basis and charged just for what they use.[20,21,22,23,24]</p>	<ol style="list-style-type: none"> 1. The user doesn't have to invest for physical infrastructure as it will be provided by IaaS on demand. So this gives fully mobility to focus on the development of applications. 2. With PaaS services application development is simple. So anyone can develop an application with less technical knowledge by using web browser. 3. User can have control over the applications that are installed within their platforms and can create a platform that suits their specific requirements. They can 'pick and choose' the features they feel as necessary. 4. In PaaS applications can be changed or modified if required. 5. The services are not isolated, application specific or location dependent. So users in various locations can work together provided they are connected through a communication medium. 6. Security of user's data and the application is the responsibility of the cloud provider. Data security, backup and recovery are the major security issues.
<p>Software as a Service(SaaS)The third cloud service model is Software as a Service which provides a platform in which the users access the software from the cloud. The users of SaaS will not have to worried about managing the cloud infrastructure and platform on which the application is running. The software installation and operation is the responsibility of the service providers and already available by using IaaS and PaaS. This is typically end user applications delivered on demand over a network on a pay per use basis. MicrosoftOffice365, Onlive, GT Nexus, Marketo, and TradeCard, google apps are some examples of SaaS. These applications are hosted in "the cloud" and can be used for a wide range of tasks for both individuals and organizations.[24,25,26,27]</p>	<ol style="list-style-type: none"> 1. No additional infrastructure or platform required to run the applications, as it provided by the service provider (IaaS and PaaS). 2. Software Applications are ready to use once the user subscribes. The user only have to pay for software not for infrastructure or platform setup. 3. With SaaS services application development is simple. So anyone can develop an application with less technical knowledge any time by using web browser. 4. Software updating is automatic i.e if any updates are available online to existing user, offered free of charges. 5. SaaS provides mobility to the user where applications can be accessed via any internet enabled device, which makes it ideal for those who use a number of different devices, such as internet enabled phones and tablets, and those who don't always use the same computer. 6. The services are not isolated, application specific or location dependent. So users in various locations can work together provided they as connected through a communication medium. 7. There are no initial setup costs is required with SaaS, as SaaS offered with other services.

Table-2: The top 10 cloud computing service providers.

SL No	Name of the Service Providers	Contribution	Services	Platform	Infrastructure details	Interfaces
1	Amazon	Amazon is one of the best business cloud service provider so far. Amazon offers services like Amazon Elastic Computer Cloud(EC2), Amazon Elastic Map reducer(EMR), Amazon Simple Storage Services(S3), Amazon virtual private cloud(VPC).[21]	Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS)	Red Hat Enterprise Linux, Windows Server 2003 R2, 2008 and 2008 R2.	1.7GB RAM, 160GB local storage, 1 EC2 Compute Unit	<ul style="list-style-type: none"> • API (Application Programming Interface) • Command Line • Graphical User Interface • Web Based Application/Control Panel.
2	IBM	IBM provides cloud computing services like IBM Blue Cloud, IBM Smart Cloud and IBM Dynamic Infrastructure which offers companies access to tools that allow them to manage large scale applications and database via IBM's Cloud.[21]	Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS)	IBM Web sphere and DB2.	One Virtual 32 bit CPUs with 1.25GHz; 2 Gb Virtual memory; 60 GB Instance storage.	<ul style="list-style-type: none"> • API (Application Programming Interface) • Web Based Application/Control Panel.
3	Google	Google's cloud services provides a platform of the gaming and mobile companies to develop their applications. Google Drive is a service for data storage.	Platform as a Service (PaaS)	Windows Mac OS X, Linux/ Other Platforms.	Based on requirements and existing environment	<ul style="list-style-type: none"> • API (Application Programming Interface) • Web Based Application/Control Panel.
4	Microsoft	Microsoft provides Windows Azure, the "cloud operating system" as PaaS. Now a days the Azure Services Platform is developed to run on the Windows Azure operating systems to give organizations access to Microsoft services like Live, .Net, SQL, SharePoint, and Microsoft's Dynamic CRM.	Platform as a Service (PaaS)	Managed code languages supported by .NET	1.6 GHz CPU, 1.75 GB RAM, 225 GB Instance Storage, Moderate I/O Performance	<ul style="list-style-type: none"> • Web Based Application/Control Panel • API (Application Programming Interface) • Command Line
5	AT&T	AT&T provides two cloud services: Synaptic Hosting, through which client companies will be able to store Windows serve, Linux client server applications and web applications on AT&T's cloud; and Synaptic Storage, enabling clients to store their data on AT&T's cloud	Platform as a Service (PaaS)	Synaptic Hosting platform virtual hosting solution.	Based on requirements and existing environment	<ul style="list-style-type: none"> • Web Based Application/Control Panel
6	Salesforce	SalesForce is also a key service provider in the cloud. It was the first one to offer a cloud service called Heroku, meant for home grown applications	Platform as a Service (PaaS), and Software as a Service (SaaS)	Supports all major development environments including .NET, Java, PHP	1.6 GHz CPU, 1.75 GB RAM, 225 GB Instance Storage, Moderate I/O Performance	<ul style="list-style-type: none"> • API (Application Programming Interface) • Web Based Application/Control Panel
7	Rackspace	It provides Infrastructure requirements for the cloud implementation	Infrastructure as a Service	Supports all major development environments	512 MB RAM, 1 vCPU, 20GB local storage, 20 Mbps public network throughput, 40 Mb	<ul style="list-style-type: none"> • API (Application Programming Interface) • Web Based Application/Control Panel
8	Orange Scape	It provides a platform as Orange scape using Cent OS	Platform as a Service (PaaS)	Supports all major development environments used in Cent OS	0.5 GB RAM, 1/2vCPU, 20 GB SATA SAN Storage, 1 TB of data transfer included.	<ul style="list-style-type: none"> • Web Based Application/Control Panel • API (Application Programming Interface) and graphical user interfaces.
9	CISCO	Cisco infrastructure services	Infrastructure as a	Based on	Based on	Web Based

		provides infrastructural requirements for cloud applications	Service	requirements	requirements and existing environment	Application/Control Panel
10	Enki Consulting	ENKI is PaaS provider of personalized cloud services. It is based on ENKI enabled infrastructure.	Platform as a Service (PaaS)	Supports all major development environments including .NET, Java, PHP	Advanced Firewall Backup Storage Data Encryption Frequent Data Back-Up	<ul style="list-style-type: none"> Web Based Application/Control Panel API (Application Programming Interface) and graphical user interfaces

Table-1(Types of cloud deployment model)

DEPLOYMENT MODEL	DIAGRAM
<p>Public Cloud(External Cloud)</p> <p>The most popular model of cloud computing to many users is the public cloud model. It provides cloud services in a virtualized environment accessible via Web applications or Web services through internet (Public Network). The cloud services and cloud resources are accessed from very large resource pools that are shared by all the end users as depicted in figure-4. It is owned by an organization selling cloud services. Cloud services like IaaS, PaaS and SaaS follows the public cloud model and gives Flexibility to end users for accessing these services from any internet enabled devices.</p>	
<p>Private Cloud(Internal Cloud)</p> <p>A private cloud provides a distinct and secure cloud based environment in which only the authentic users within an organization can access, as depicted in figure-5 N4 acts as a private cloud terminal. It makes the use of virtualization within the private area. It is provided and managed by the organization or a third party, and can be deployed according to the requirement.</p>	
<p>Community Cloud(Grouped Cloud)</p> <p>A community cloud provides a distinct and secure environment where organizations with similar requirements share a common cloud infrastructure. So it is called as generalization of a private cloud where a private cloud infrastructure is only accessible to permissible users as shown in the figure-6. It is provided and managed by the organization or a third party, and can be deployed according to the requirement.</p>	
<p>Hybrid Cloud(Mixed cloud)</p> <p>A hybrid cloud provides an integrated environment accessible to both private and public cloud functionalities. For better utilization of resources an organization can deploy public cloud services along with private cloud this can be achieved by registering private cloud services to a public cloud service. The figure-7 shown below is the deployment model for hybrid cloud.</p>	

Redundancy.

Consider how redundant your provider's systems are. That helps for data replications and data migration in case of database failure.

Maintenance.

One of the nicest aspects of using a cloud is that the provider handles the maintenance. But users should know, when providers will do maintenance tasks:

- a. Will services be unavailable during that time?
- b. Will services be available, but with much lower throughput?
- c. Will the consumer have a chance to test their applications against the updated service?

Data location.

There are regulations that certain types of data can only be stored in certain physical locations. Providers can respond to those requirements with a guarantee that a user's data will be stored in certain locations only and the ability to audit that situation.

Data seizure.

If law enforcement seizes a provider's equipment to capture the data and applications belonging to a particular registered users, that seizure is likely to affect other users that use the same provider. Consider a third party to provide additional backup.

Provider failure.

Make contingency plans that take into account the financial health of the provider.

Jurisdiction.

Again, understand the local laws that apply to your provider as well as you do the laws that apply to you.

Brokers and resellers.

If your provider is a broker or reseller of cloud services, you need to understand the policies of your provider and the actual provider. The figure-3 shown below gives a clear idea regarding the trust based SLA model for cloud environment.

A trust based SLA model for cloud environment

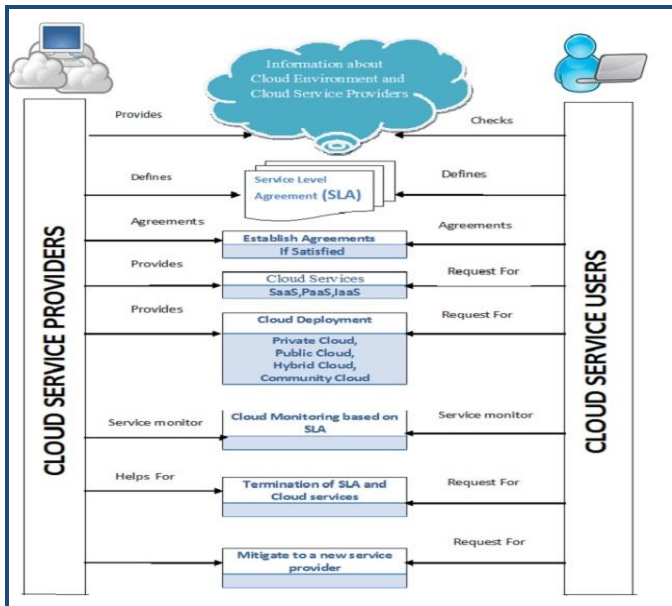


Figure-3 (Trust based SLA model)[8]

Cloud computing service models.

Based on the usages of data and applications cloud computing services are broadly classified in three different types (Infrastructure as a Service (IaaS) , Platform as a Service(PaaS), Software as a Service(SaaS)) called as cloud service models. [17,18,19,20] A layers of cloud computing service model and their infrastructural requirements and explanation about all the three is available in the table-1.

Cloud Service Management

Cloud Layer	Service Models		
	IaaS	PaaS	SaaS
Data			
Interfaces (APIs, GUIs)			
Applications			
Solution Stack (Programming languages)			
Operating Systems (OS)			
Virtual Machines			
Virtual network infrastructure			
Hypervisors			
Processing and Memory			
Data Storage (hard drives, removable disks, backups, etc.)			
Network (interfaces and devices, communications infrastructure)			
Physical facilities / data centers			

Figure-5 cloud computing service responsibilities[12]

Cloud Service Providers

Cloud service providers(CSP) are utility computing provider organizations that delivers cloud computing based services and solutions to the cloud users . The services includes Virtual infrastructure, computing platforms and applications software.CSP delivers cloud services through on-demand, pay-as use systems as a service to cloud users. Users access cloud resources through web based applications. A user will choose a good cloud service provider based upon the services, platforms, Infrastructure details and user interfaces.[28] A list of top 10 cloud service providers is given in table-2

Cloud Deployment Models

According to the usages of data and applications required by the users the cloud computing models are broadly classified in four different types called as cloud deployment models. [27,29-32] details Cloud deployment models is available in table-3

Conclusion

Understanding the roles of the cloud service providers and cloud users is important for the service level agreement (SLA).Providing security and privacy in the cloud computing environment and developing efficient and effective solutions for it is really a difficult task for the cloud service providers. Confidentiality, integrity, reliability and availability are widely used terminology based upon which the cloud users rely on the service providers. In this paper we have discussed about the service level agreements(SLA) and cloud computing models in details from the service providers as well as the cloud user point of view.

References

- [1]. Wikipedia, http://en.wikipedia.org/wiki/Cloud_Computing
- [2]. Rafael Moreno-Vozmediano,Rubén S. Montero, Ignacio M. Llorente, " Key Challenges in Cloud Computing -Enabling the Future Internet of Services", Published by the IEEE Computer Society 1089-7801/13/ © 2013 IEEE, IEEE internet computing
- [3]. M.Rajendra Prasad, R. Lakshman Naik, V.Bapuji, " Cloud Computing : Research Issues and Implications ", International Journal of Cloud Computing and Services Science (IJ-CLOSER) Vol.2, No.2, April 2013, pp. 134~140 ISSN: 2089-3337.
- [4]. Francesco M.A and Gianni F. "An approach to a cloud Computing network", IEEE, August 2008, pp113-118
- [5]. Huaglory Tianfield,"Cloud Computing Architectures", 978-1-4577-0653-0/11/©2011 IEEE.
- [6]. S. V. Kavitha, "A survey on security issues in service delivery models of cloud computing" Journal of Network and Computer Applications, Elsevier, vol. 34, (2011), pp. 1–11.

- [7]. P. Adams, "Advantages and Disadvantages Of Cloud Computing System", *Advantages And Disadvantages Of Cloud Computing System*, (2011) November 18.
- [8]. Shakeel Ahmad, Bashir Ahmad, Sheikh Muhammad Saqib, Rashid Muhammad Khattak "Trust Model: Cloud's Provider and Cloud's User " *International Journal of Advanced Science and Technology* Vol. 44, July, 2012
- [9]. Marco Comuzzi, Guus Jacobs, Paul Grefen "Clearing the Sky - Understanding SLA Elements in Cloud Computing" *Beta Working Paper series* 412
- [10]. Linlin Wu, Rajkumar Buyya "Service Level Agreement (SLA) in Utility Computing Systems", *Cloud Computing and Distributed Systems (CLOUDS) Laboratory*
- [11]. Wikipedia, http://en.wikipedia.org/wiki/Service_Level_Agreement
- [12]. <http://www.cosentry.com/information-center/who-is-cosentry/certifications/pci-dss-compliance>
- [13]. Mitchell Cochran, Paul D. Witman "Governance and service level agreement issues in a Cloud computing environment" *Journal of information technology management* ISSN #1042-1319 A publication of the association of management
- [14]. Pankesh Patel, Ajith Ranabahu, Amit Sheth, "Service Level Agreement in Cloud Computing" *Knoesis Center, Wright State University, USA*
- [15]. Jessica McCarthy, "Service Level Agreements for Cloud Computing" ISBN 978-1-4614-1 - e-ISBN 978-1-4614-1 - DOI 10.1007/978-1-4614-1 - Springer New York Dordrecht Heidelberg London Library of Congress Control Number: 2011939783 © Springer
- [16]. C. Robert, "Cloud Computing: Advantages and Disadvantages", <http://boardroombrief.com/2010/08/cloud-computing-advantages-and-disadvantages/>, (2010) August 24
- [17]. Xu Xiaoping, Yan Junhu, "Research on Cloud Computing Security Platform", 978-0-7695-4789-3/12 © 2012 IEEE DOI 10.1109/ICCIS.2012.238.
- [18]. Dimitrios Zisis, Dimitrios Lekkas, "Addressing cloud computing security issues", 0167-739X/ © 2010 Elsevier B.V. All rights reserved. doi:10.1016/j.future.2010.12.006.
- [19]. "Understanding Cloud Computing Vulnerabilities", by the IEEE Computer and Reliability Societies 1540-7993/11/ © 2011 IEEE March/April 2011.
- [20]. Hassan Takabi, James B.D. Joshi, Gail-Joon Ahn, "Security and Privacy Challenges in Cloud Computing Environments", by the IEEE Computer and Reliability Societies, 1540-7993/10/ © 2010 IEEE, November/December 2010.
- [21]. Zhifeng Xiao and Yang Xiao, *Senior Member, IEEE*, "Security and Privacy in Cloud Computing", *IEEE Communications Surveys & Tutorials*, Vol. 15, No. 2, second quarter 2013, 1553-877X/13/c_2013 IEEE.
- [22]. Peter Mell, "What's Special about Cloud Security?", *IT Pro* July/August 2012, Published by the IEEE Computer Society, 1520-9202/12/ © 2012 IEEE.
- [23]. Jianhua Che, Yamin Duan, Tao Zhang, Jie Fan, "Study on the security models and strategies of cloud computing", 1877-7058 © 2011 Published by Elsevier Ltd. doi:10.1016/j.proeng.2011.11.2551.
- [24]. Xue Jing, Zhang Jian-jun2. "A Brief Survey on the Security Model of Cloud Computing" 978-0-7695-4110-5/10 © 2010 IEEE DOI 10.1109/DCABES.2010.103
- [25]. Engr: Farhan Bashir Shaikh, Sajjad Haider, "Security Threats in Cloud Computing", 978-1-908320-00-1/11@2011 IEEE
- [26]. H.Sato, et al., "A Cloud Trust Model in a Security Aware Cloud", *SAINT2010*, pp.121-124.
- [27]. Mladen A. Vouch, "Cloud Computing Issues, Research and Implementations", *Journal of Computing and Information Technology - CIT* 16, 2008, 4, 235-246
- [28]. [www.http://webhosting.about.com/od/Clouding-Hosting/a/Top-10-Cloud-Computing-Vendors.htm](http://www.webhosting.about.com/od/Clouding-Hosting/a/Top-10-Cloud-Computing-Vendors.htm)
- [29]. Latifa Ben, Arfa Rabai, Mouna Jouini, Anis Ben Aissa, Ali Mili, "A cybersecurity model in cloud computing environments", 1319-1578 © 2012 King Saud University. Production and hosting by Elsevier B.V. All rights reserved. <http://dx.doi.org/10.1016/j.jksuci.2012.06.002>.
- [30]. M. Mackay, T. Baker, A. Al-Yasiri, "Security-oriented cloud computing platform for critical infrastructures", 0267-3649/2012 M. Mackay, T. Baker & A. Al-Yasiri. Published by Elsevier Ltd. All rights reserved. <http://dx.doi.org/10.1016/j.clsr.2012.07.007>.
- [31]. S. Subashini, V.Kavitha, "A survey on security issues in service delivery models of cloud computing", 1084-8045/2010 Elsevier Ltd. All rights reserved. doi:10.1016/j.jnca.2010.07.006.
- [32]. Y. Jianfeng, C. Zhibin. "Cloud Computing Research and Security Issues" *CISE* 2010. Dec, 2010
- [33]. Ashish Kumar, "World of Cloud Computing & Security", *International Journal of Cloud Computing and Services Science (IJ-CLOSER)* Vol.1, No.2, June 2012, pp. 53-58 ISSN: 2089-3337.
- [34]. Wenjuan FAN, Shanlin Yang, Jun Pei, He Luo, "Building trust into cloud", *International Journal of Cloud Computing and Services Science (IJ-CLOSER)* Vol.1, No.3, August 2012, pp. 115-122 ISSN: 2089-3337.
- [35]. simulation. In *Proceedings of the 2011 Military Modeling & Simulation Symposium (MMS '11)* (2011). Society for Computer Simulation International, San Diego, CA, USA, 92-100.
- [36]. Hemraj Saini, T. C. Panda, Minaketan Panda. 2011. Prediction of Malicious Objects in Computer Network and Defense", *International Journal of Network Security & Its Applications (IJNSA)*, Vol.3, No.6, pp.-161-171, 2011.
- [37]. S.B.Dash, H.Saini, T.C.Panda, A.Mishra, "Prediction of Trustworthiness in the Cloud Computing Environment using Predator-Prey Model", *International Journal of Cloud Computing and Services Science (IJ-CLOSER)* Vol.2, No.5, October 2013, pp. 336-344 ISSN: 2089-3337