ijecs open access www.ijecs.in

International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume - 3 Issue - 8 August, 2014 Page No. 7718-7722

Trust Understanding in Cloud and It's Services

[1]Sushil Malik, [2]Shalini Singh, [3]Jyoti Rajpoot,[4]Richa Parashar

Abstract :— The Cloud can be considered as a platform or infrastructure that is responsible for execution of services and applications in a reliable and elastic fashion with predefined quality parameters to provide more Availability, agility, adaptability, reliability etc. In Brief, 'cloud' is an elastic execution environment of resources involving multiple stakeholders and providing a metered service at multiple granularities for a specified level of quality (of service). There are various services provided by cloud service providers to their users such as Saas, Pass, Iaas, these services are available to the cloud users depend upon some trust agreement across the globe. Trust is the another factor which is one of the most challenging issue in the cloud computing area for which various models has been proposed in last few years. The objective of this paper is to impart a clear idea about various services provided by cloud, there comparative approach and the role of various trust mechanism in cloud.

Key-words— Cloud, Cloud service providers, IaaS, PaaS, SaaS, SLA, Operating System, Trust.

1 Introduction

1.1 Definition of Cloud-Computing

The most widely used definition of the cloud computing model is introduced by National Institute of Standard Technology as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g. network, servers, storage, application, and services) that can be rapidly provisioned and released with minimal management effort or services provider interaction. "Cloud Model has two characteristics which are Multi-tenancy and elasticity. Multi-tendency is responsible for sharing of same services within different tenants. Elasticity is responsible for scaling up and down the resources which are allocated to a service based on the current demand of that service. Both of these characteristics focus on improving the resource utilization, cost and service availability [1]. Cloud Computing is the new way of using Computing Resources just like Computers, Data Bases, Infrastructure etc. It changes the method of organizing and maintains the Computing, Services and Technologies and enables the Infrastructure which is treated as service. The cloud services are cost effective and improve scalability, reliability and agility [2].

2 Trust in Cloud-Computing

Literally we can say 'TRUST' is a mental state comprising: [3] expectancy - where trustier expects a specific behavior from the trustee (Means providing valid information or effectively performing cooperative actions); (4) belief- the belief of trustier that the expected behavior will occur, based on the evidence of the trustee's competence, integrity, and goodwill;(5) willingness to take risk - the trustier wants to take risk for that belief.

3 Requirements for Trust Mechanism:

When critical resources of user aren't on the physical territory of the user, they would have to devise mechanisms to ensuring the security and integrity of resources. To use cloud computing, users are putting their resources on cloud service provider's data centers; hence, providers need to implement the security and reliability mechanisms in behalf of their users. Furthermore, cloud computing model results into some new security threats such as fate sharing, resource sharing and data lock in. Due to these risks, users are preventing them to use cloud computing. To eliminate these risks, cloud service providers should identify main user's concerns and try to mitigate these concerns [6]. They should recognize the importance of building users' trust, different researchers proceeded to identify and analyze the elements which are important in cloud computing trust model. In order to allow customers and users of services that are used by multiple customers Cloud providers must produce enough reliable information to their customers[7].

4 Services over the Cloud:

Usually Cloud providers centre on one type of cloud functionality provisioning: Infrastructure, Platform or Software / Application, though there is no restriction to provide multiple types of services simultaneously, that can often be observed in PaaS (Platform as a Service) providers. PaaS providers offer specific applications, such as Google App Engine along with Google Docs. Because of these combinatorial capabilities they are also referred as "Components" Terminology applied are slightly differ than literature and publications due to the fact that area of some application overlap and it is difficult to distinguish. Let us take an example, platforms provides access to resources indirectly, sometimes it is confusing with infrastructures.

5 Types of services:

5.1 Software as a Service (SaaS):

Software as a Service (SaaS) can be considered as deployment with an alternative to software licensing. In SaaS service providers are responsible for delivering, managing of applications remotely with the help of one or more providers over the intranet and provides their customers on demand services like electricity bill [8]. Users can run applications directly from SaaS providers web servers and they can run at their end and they can disable that application after use or after the on-demand contract expires. In Brief, it is data centers of clouds service providers hosted the software and data associated with them.

5.2 Platform as a Service (PaaS):

PaaS provides its customers the luxury of deploying applications, software or programs without the burden of purchasing and maintaining the underlying hardware and software. It comes above IaaS in stack of cloud. PaaS offers facilities of deployment, testing, application development and hosting of services such as data integration, service integration, team collaboration, scalability, state management, storage, security, application versioning, and persistence and developer community facilitation. Users required building the application in compliance with the platform vendor's specification, while the networks, servers, storage and other services are provided by the platform vendor. As all the underlying requirements are handled by a single vendor, it helps you to efficiently manage the software deployment process without encountering unexpected delays or issues. [9]

5.3 Infrastructure as a Service (IaaS):

It is also referred to as Resource Clouds, provide (managed and scalable) resources as services to the user – in other words, they basically provide enhanced virtualization capabilities and directly attached to the hardware in clod stack. Iaas provides computer infrastructure in the form of a service and to accomplish that different resources are provided via a service interface: Data & Storage Clouds responsible for reliable access of data of potentially dynamic size, weighing resource usage with access requirements and/or quality definition. Examples: Amazon S3, SQL Azure [10].

5.4 Human-as-a-Service (HuaaS): This is the scenario where human intelligence is used in contribution of services. These services can be viewed as predictive events, popular news, and popular ideas. These services are based on popular opinion of the population. Every individual among the crowd can use any tool of the technology to solve the task.

6 Implementation Issues in Cloud:

6.1 Privacy:

Privacy is in various forms like "control of information about us". Computing data is stored and processed remotely in cloud so subscribers always worried about privacy. Cloud services runs on those servers or machines about them subscribers are not aware which results into the privacy issues and fear of leakage or loss of commercially sensitive data. Top database vendors are adding Cloud support for their databases like Oracle can now run directly on Amazon's Cloud service platform (EC2).

6.2 Security:

Cloud service providers provide data storage by transmission encryption, authorization user authentication hence their users worry about vulnerability of data to the thieves, hackers and disgruntled employees. In most of the cases the uniqueness of cloud security is helpful in protecting data because it cannot be recognize easily. Many technologies are used by cloud service providers like encryption, digital signature, firewalls, virtual environments etc.

6.3 Reliability:

Reliability can be viewed as a cloud service provider is financially stable or not. Most of the cloud providers attempt to overcome the concern of their subscribers by providing redundant storage techniques. But still there are chances that a service can crash or go out of business, leaving users with limited or no access to their data.

6.4 Data portability and conversion:

Some of Cloud users are assume that when they would have to transfer data during switching providers they would face difficulty and security breaches. Because Porting and converting data is highly dependent on the nature of the Cloud provider's data retrieval format, particular in cases where the format cannot be easily discovered.

6.5 Intellectual property:

Intellectual property is the individual invention of Cloud service provider. The concern arises, is that invention is patentable? Or cloud providers have claim on their invention.

7 Aspects of Trust

7.1 Trust based on Reputation:

Reputation of entity is aggregated opinion of a community towards the same, but trust is between two entities. Both these terms are related but convey different meaning. In the same community, high reputed entity is trusted by many entities. Those entities which need to make trust may use reputation to calculate to estimate the trust level of trustee.

Researchers in computer sciences have exploited the benefit of all these studies as they provide vital insight into human behavior under various circumstances. The role of trust and reputation in open, public distributed systems such as e-commerce, peer to peer networks, grid computing, semantic web, web services and mobile networks have been studied by several researchers [11]. Reputation depends in the high grade of user's wishes. Company and individuals must request theses services to the cloud computing vendors [12].

7.2 Service level Agreement based trust:

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 provides 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. 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 [13].

7.3 Trust Based on Policy of the organization:

Policy as Trust management (PocT) is one of the most popular and traditional ways to establish trust among parties and has been used in cloud – environment [14]. It is a widely used mature technology that employs "formal trust" mechanism to support digital signature.

7.4 Evidence-Based trust:

For an appropriate treatment of application-level interactions among autonomous and adaptive parties, an evidence-based account of trust is essential. Key examples are service-oriented computing and social networks. Existing approaches either ignore evidence or only partially address the twin challenges of mapping evidence to trustworthiness and combining trust reports from imperfectly trusted sources, trust arises in two main settings studied in economics [Dellarocas 2005]. In the first, the agents adjust their behavior according to their payoffs. The corresponding approaches to trust seek to alter the payoffs by sanctioning bad agents so that all agents have an incentive to be good. In the second setting, which this paper considers, the agents are of (more or less) fixed types, meaning that they do not adjust whether their behavior is good or bad. The corresponding approaches to trust seek to distinguish good agents from bad agents, i.e., signal who the bad (or good) agents are. Of course, the payoffs of the agents would vary depending on whether other agents trust them or not. Thus, even in the second setting, agents may adjust their behavior. However, such incentive-driven adjustments would occur at a slower time scale [15].

7.5 Trust as a service (SOA) framework:

SOA and web services are one of the important enabling technologies for cloud computing in the sense that resources are exposed in clouds as services.[16] RSA announced the Cloud Trust authority (CTA) as a cloud service, called Taas (trust as a service), to provide a single point of configuration and managing security of cloud services from multiple providers. Taas includes identity service, enabling single sign on multiple cloud providers against a common benchmark.

8 Comparative approach of Iaas, SaaS and PaaS:

Infrastructure-as-a-service (IaaS) is at the lowest level and pre-configured hardware is provided via a virtualized hypervisor, high level infrastructure such as operating-system must provided by buyer with their virtual applications which enhance their virtual capabilities. Besides, PaaS includes operating system and application services, you would be required to build the application in compliance with the platform vendor's specification, while the networks, servers, storage and other services are provided by the platform vendor while in SaaS applications are owned, delivered and managed remotely by one or more providers over the Internet or an intranet, and licensed to customers as an on-demand service. SaaS is used where users system are less configured only basic operating system installed on them everything is on-demand over the cloud while in Paas we can deploy our own applications but it is quite expensive to manage by themselves.

9 Discussion and Conclusion:

Understanding the roles of the cloud service providers and cloud users is important for the trust mechanisms used in different services of cloud. To provide security and privacy in the cloud computing is a difficult task for service providers. In this article we have presented a comprehensive survey to the best of our knowledge first to focus on the services of the cloud-computing environment and their trust mechanisms for security, acceptability, and reliability of cloud users. We distinguish various cloud services by each other. In future we will design a framework which will justify most of the important trust mechanisms.

References:

1. A New Technique of Data Integrity for Analysis of the Cloud Computing Security, 2013 5th International Conference on Computational Intelligence and Communication Networks
2. REVIEW OF CLOUD TESTING, TYPES, CHALLENGES AND FUTURE SCOPE, International Journal Of Advance Research In Science And Engineering http://www.ijarse.com IJARSE, Vol. No.2, Issue No.5, May, 2013
3. Michael B (2009) In clouds shall we trust? IEEE Security and Privacy 7: http://dx.doi.org/10.1109/MSP.2009.124 [3]
4. Everett C (2009) Cloud computing: A question of trust. Computer Fraud Security 2009(6): 5–7. http://dx.doi.org/10.1016/S1361-3723 (09)70071-5
5. Garrison G, Kim S, Wakefield RL (2012) Success factors for deploying cloud computing. Commun ACM 55(9): 62–68. http://doi.acm.org/10.1145/2330667.2330685
6. A Model for User Trust in Cloud Computing, Ahmad Rashidi and Naser Movahhedinia International Journal on Cloud Computing: Services and Architecture(IJCCSA),Vol.2, No.2, April 2012
7. BUILDING CUSTOMER TRUST IN CLOUD COMPUTING WITH TRANSPARENT SECURITY, White Paper November 2009
8. URL: http://www.esi.mil/saas_toolkit/saas_definition.html
9. URL:http://blog.qburst.com/2013/06/the-future-of-hosting-platform-as-a-service-paas/
10. Expert Group Report Public Version 1.0 Rapporteur

for this Report: Lutz Schubert [USTUTT-HLRS] Editors: Keith Jeffery [ERCIM], Burkhard Neidecker-Lutz [SAP Research]

11. Trust Management in Cloud Computing: A Critical Review , Mohamed Firdhous, Osman Ghazali and Suhaidi Hassan, International Journal on Advances in ICT for Emerging Regions 2011 04 (02) : 24 - 36. [11]
12. Reputation in Cloud Computing, Adrian Yanes, Aalto University, School of Science and Technology
13. Service Level Agreement Assurance in Cloud Computing: A Trust Issue, by 2899-2906,S.B.Dash, H.Saini , T.C.Panda, A. Mishra, (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014
14. Trust Management of Services in Cloud Environments: Obstacles and Solutions by TALAL H. NOOR1, QUAN Z. SHENG1 The University of Adelaide and SHERALI ZEADALLY2 University of the District of Columbia and JIAN YU3 Swinburne University of Technology.
15. Evidence-Based Trust:A Mathematical Model Geared for Multiagent Systems by YONGHONG WANG Carnegie Mellon University and MUNINDAR P. SINGH North Carolina State University.
16. Trust as a Service: A Framework for Trust Management in Cloud Environments by Talal H. Noor and Quan Z. Sheng School of Computer Science, The University of Adelaide, Adelaide SA 5005, Australia {talal,qsheng}@cs.adelaide.edu.au