International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org
Volume 4, Issue 1, January-February 2015 **ISSN 2278-6856**

BUILDING TRUST IN CLOUD: COMPARISON OF MECHANISMS

[1]ANKITA SHARMA, [2]PARUL PAL

[1]DEPARTMENT OF COMPUTER SCIENCE, JIMS ,ROHINI ,GGSIPU

[2]DEPARTMENT OF COMPUTER SCIENCE, JIMS ,ROHINI ,GGSIPU

ABSTRAC

Cloud computing, nowadays is gaining wide acceptance by the business enterprises. However, despite gaining acceptance and having several advantages there have been issues related to building of trust when the end user hands over the crucial operations of enterprise to another party in the hope that this party will safely upkeep the company's belongings. This paper addresses the issues of building the trust in the cloud wherein the end user is assured of the fact that when he is giving the company's belongings to another party it is safe and secure. The design of the paper follows a structured approach. It starts with the basics of setting the background for cloud computing, further moving down to dealing with the structure of cloud and then gradually moving on to the process of defining trust and the various types of trust that can be deployed. Finally, the paper concludes with the limitations as to how it can be further utilized in the process of building trust.

Keywords: Cloud, Infrastructure, Reputation, Trust

1. Introduction

Nowadays, business organizations are demonstrating an inclination towards Cloud Computing. Cloud computing in essence, is relatively a new concept but it has taken the world by storm on account of several benefit it offers to the business units in terms of leveraging time and cost which are core drivers of business. Worth mentioning is the fact that business units are in the throes of hyper competitiveness and as such they are required to operate on 24x7x365 time slot so as to survive in the market. Thus, business units or business organizations have been ardently looking for technological solution (or solutions) which can assist them to leverage time and cost and at the same time enable them to achieve business objective. Cloud computing technology has provided them the solution to which they were looking for.

Cloud computing, in essence, comprises of three layers of components viz. Infrastructure, Platform and Application[3]. These three components are commonly referred to as IAAS, PAAS and SAAS. In the terminology of cloud computing, IAAS is referred to Infrastructure as service, PAAS is referred as Platform as a service while SAAS is known as Software as as Service. The term service is concomitantly used on account of the fact that the end-user pays for what he consumes. Thus, if an end-user is consuming infrastructure then the service provider is charging for the usage based on terms and condition. In a similar manner, if the end user is utilizing the services of platform or software, he is paying for what the end user is computing. Thus, in a nutshell, cloud computing is outsourcing of data center.

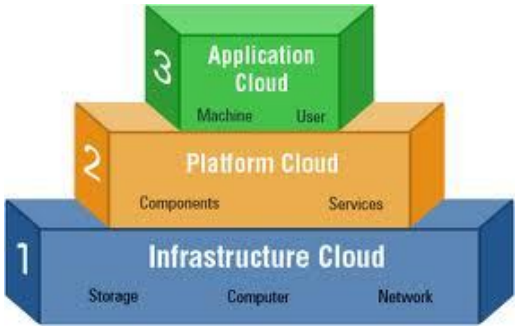

Fig 1, below depicts layers or components of cloud. With this approach of pay what you consume, business units stand to gain immensely in terms of time and cost. For, example, if a business unit wants to avail the service of a particular software he is required to pay to the service provider based on the terms and conditions.

With cloud computing rapidly gaining popularity in terms of pay for what you use, with no frills attached to maintenance of infrastructure or platform or software, certain issues have emerged lately and which nevertheless are indeed genuine. The issue of safety and security of data which the end user generates or maintains on the cloud while availing the services of the cloud. Or in other words, issues related to building of trust with the service provider. This paper is concerned with the process of building trust in clouds and comparison mechanisms for building trust. The design of the paper follows a structured approach. Section 1 of the paper starts with the background by setting the scope for the development of the importance of cloud computing in today' highly competitive business world. It also covered a brief reference to the structure of cloud by highlighting the basics of working mechanism with service provider. Section 2 covers the process of defining trust and various nuances associated with trust. Section 3 covers metrics related to trust.

2.Related Work

In plain common parlance, trust is defined as the generation of feeling of assurance, or confidence by one party onto another party who are somewhat bounded by certain terms or conditions which may be oral or written. Thus, when it comes to the commercial transactions this boundedness is provided by contractual agreement followed by service level agreements or SLA's. Thus, in the case of cloud computing services, the contract binds or

bounds the service level provider and the end user. While dealing with cloud computing issues, trust is considered to be the focal point. Of late there has been issues where safety and security of end user data has been compromised forcing the parties go into litigation. Due to complexity in the structure of cloud based technology it is not the data alone that needs to be taken care off, there are several other points of consideration which are required notably among them are the uptime of server in case of failure; issues pertaining to quality of data; loss of data during data uploading and data migration ; data leakage and the like.

This paper is concerned with the process of building trust at the infrastructure level of the cloud. In order the address the issues related to building of trust at the IAAS level, let us dwell on the basics of IAAS.

In the case of IAAS, the computing resource that is provided to the end user is virtual hardware or in other words this is the infrastructure that is given by the service provider. Apart from this virtual disk space, the end user is provided with virtual server space, network connection, the associated bandwith, the IP address and the like. This is similar to the process of pulling hardware from the pool of several servers and networks which are generally distributed across several data centers which are managed by the service providers. The end user on the other hand is provided access build its own IT platform for carrying out several operations.

With this generalized concept of IAAS in place, let us now look to the aspect where the trust needs to built up at the infrastructure level. Further, this paper limits the scope to handling data at the server. Thus, the scope of the paper is limited to data handling at the infrastructure level.

In the case of data handling, trust can be evaluated (and consequently these factors ensure building and maintenance of trust) on the points enumerated below. (Figure 2)

Reputation of service provider

Perhaps this is the most important factor which is responsible for building trust with end user. The vendor whose reputation has been excellent has a very high trust in the market as well as with the clients. However, worth mentioning is the fact that for further scope of research, the word reputation needs to be narrowed down immensely. For example, a vendor may have a reputation for agreeing to the terms and conditions of SLA whereas it does not have good reputation for meeting the committed service of server uptime as it does not fall under the SLA

Attributes of data

This is another method which is used to evaluate and thus build trust. This factor basically deals with the attributes of data. This in essence means how the service provider (and consequently the end user) views the data and how he manages it i.e. Is the data of confidential in nature; or is the data required to be addressed and accessed by all end user of the enterprise; or is the data transient in nature and is thus required to be backed up ofter; and the like.

Self assessment of the various operations or contractual agreements executed with the service provider

This is another important factor, and which nevertheless is the most crucial factor which assists in the development of trust. The end user has to have a pro-active role in the process of building trust. Or in other words, the end user must ensure that all contractual agreements are being executed as the terms and conditions. Any deficiency on the performance is liable to ensure that there is some loss of trust and in extreme cases canceling of the contract and legal issues.

Meeting applicable government laws and policies

This is another factor which is responsible for building trust. This essentially means that the service provider should adhere to the applicable rules and regulations of the government and thus should not indulge in any illegal activities.

3. Trust Metrics

In the previous section, we covered the various factors on which the trust is built. We also saw that trust has two components *viz.* The end user *and* the service provider. Consequently, in section two we had covered the factors on which the end user evaluates the service provider and the means through which the service provider can build trust.

In this section we will cover the metrics related to trust s the metrics are driving force for maintaing trust.

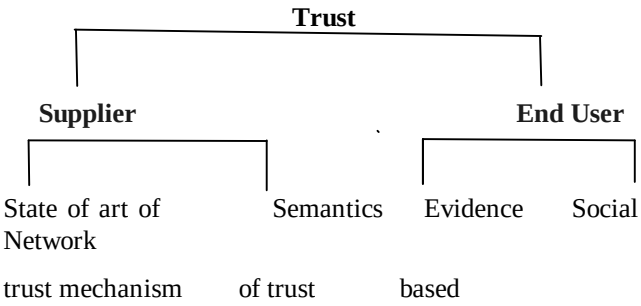

Fig 2 The following gives the various trust metrics can be utilized for building trust in cloud

State of Art of Trust

This includes Reputation based trust. This metrics assists the end user to choose a service of the cloud. While chosing the service, the SLA is developed to adhere to the process of strengthening of trust between the provider and user. The same has been expressed by Ziegler CN, Lausen G [3], describes trust as a mental state comprising: (1) expectancy – this includes the expectation of the trustor from the trustee. (2) belief- the trustor believes that the expected behavior occurs, based on the evidence of the trustee's competence, integrity, and goodwill (3) willingness to take risk - the trustor is willing to take risk for that belief.

Jingwei Huang [2] further classifies trust into two types: **trust in performance and trust in belief.** The trustee's performance is considered as the truth of what the trustee says. For example if x is considered as to what the trustee states; for the second, x represents a successful performance, which is considered as a statement that the trustee made, which describes his or her performance. **A trust in performance relationship, trust_p(d,e,x,k),** represents that d trusts trustee e and also e's performance x is generated in context k. This relationship means that if x is made by e in context k, then d has a belief that x in that context.

trust_p(d,e,x,k)≡madeBy(x,e,k)⊃believe(d,k⊃.x) (1)

where ⊃. is an operator for reified propositions. A trust in belief relationship, trust_b(d,e,x,k), represents that the trustor d trusts the trustee e in regards e's belief (x) well in context k. This means that if e believes x in context k , then d also believes x in the same context.

trust_b(d,e,x,k)≡believe(e,k⊃.x)⊃believe(d,k⊃.x) (2)

Trust in belief is transitive i.e. It moves down the hierarchy while trust in performance is non transitive. From the definition as given above, the trustor's mental state of belief in his expectancy on the trustee is dependent on the evidence about the trustee's competency, integrity, and goodwill. This leads to logical structures of reasoning from belief in evidence to belief in expectancy.

Evidence based Trust

Evidence based trust includes several attributes which form an input to the process of building trust based on the available evidence. For example, a client intending to avail the services of a provider needs to view i.e. Needs to convinced about the credentials of the provider through certificates, accolades and the like. These certificates, accolades form the attributes, as mentioned above.With these metrics once can be assisted in the development of trust on the basis of performance,security and privacy, accolades, certificates and the like.

Further, trust can be viewed as a mental state which comprises of (1) expectancy (2) belief and (3) willingness to take risk Mathematically, evidence based trust can be developed as follows:

believe (u,attr$_1$ (s,v$_1$)) ^….^ believe(u, attr$_n$ (s, v$_n$)) - trust_*(u, s, x ,c) (3)

Which implies that if an individual u believes a subject s has attribute attr$_1$ with value v$_1$, attribute attr$_n$ with value v$_n$ then u trusts s w.r.t x ,the performance of s or information created or believed by s, in a specific context c. For example, the certificate or accolades, as discussed above, may be given in terms of context say on time delivery or 100% compliance to SLA regarding uptime of server Also, an entity's belief in the assessment of an attribute is dependent on whether an entity trusts the entity who makes that attribute assessment. For example, in the above case, whether the certifying agency who provides accolades or certificates is itself trustable or not. This can depicted mathematically as

trust_p(u,a,attr(s,v),c) ^ madeBy(attr(s,v),a,c) ^ inContext(c)→believe(u,attr(s,v)) (4)

which states that if an individual u trusts an attribute authority a to make assertions about a subject s has attribute attr with value v in a specific context c, a specific assertion attr(s,v) is made by a in context c, and the context c is the case, then u will believe that assertion. In the formula,attr(s,v) is a reified proposition represented as a term. As not only the attributes of the cloud service are to be assessed and certified, but also the attributes of a cloud entity are required to be assessed and certified and certified. The formula, given above, may use attr(e,v) to state that cloud entity e has attribute attr with value e. In this way, a logic formula similar to (4) can describe the relation from trust in a cloud auditor to the belief in the certified attribute of a cloud entity like service provider.

Social Trust

This kind of trust includes trust which is visible or demonstrated in the social networks. This metric assists the end user on the basis of other people's opinion.

Trust In Social Networks

In case of social networking an individual is placing trust on another individual's machine with the context frame being security of data. A no of business units have come up in the form of cyber cafe, which, have built trust with their customers, in the form of verification of credentials of the customer before they are allowed to access the system. This mechanism helps to trace their customers, in case, if an individual has attempts to violate social security websites such as posting comments of morphed images on the websites.

Audit based trust mechaism

This is another important mechanism which is utilized in the process of providing evidence as well as performance based operations. The third party audits are itself a proof of the depolyement of basic processes which can support ample evidence in the process of building trust.

Comparison of trust mechanisms

Having understood the process of building trust in the cloud let us now compare the various mechanism used to build trust

Trusted Virtual Environment Module (IAAS)	LOBOT (SAAS)	Private Virtual Infrastructure
This is implemented as a part of the system. Hence cannot be implemented in standalone devices	Lobot is designed specifically to build trust in Private Virtual Infrastructure. Hence can be implemented in standalone devices	Trust is build by sharing of the responsibility between client and the service provider. Hence can provide the stand alone platform which will build trust
Can build trust based on the reputation, performance hence as it can be customized according to the needs of the customers	Can build trust on the security and performance issues as it can be customized according to the demands of market and business units	Can build trust asper the SLA. Hence the SLA becomes the guiding principle for building trust
This is designed to provide the trust to the infrastructure components of the system.	Lobot is designed to focus on providing trust worthiness to computing platform	It needs to build trust on the issue of providing transparency to the client
Can only provide the trust related to hardware security features	Can build trust in the provision for migration and monitoring of the data	Can build or provide trust related to the platform as per the Service level agreements with he client

Limitation of the paper

Though the author has tried to cover the basics of the process of building cloud, however, there are limitations. These limitations are in the form of those aspects which cannot be envisaged during the course of day to day operations for example, data which has been destroyed by natural calamity such as fire and how the service provider addresses those issues. Others example includes cases such as software which was earlier running on previous version is now no longer supported by the provider. These are separate topics and form the future scope of study.

4.Conclusion

This paper addressed the basic concepts of the cloud and the types of trust that are implemented in cloud as used in industry. With cloud computing gaining wide acceptance, the trust building mechanisms that have been addressed will become more and more refined as the volume of the work on the cloud will increase due to several advantages. These advantages will form a separate scope of study.

References

[1] Django Armstrong , Karim Djemame,http://www.comp.leeds.ac.uk/ukpew09/papers/18.pdf ‘

[2] http://www.luitinfotech.com/kc/what-is-cloud-computing.pdf

[3] http://www.dialogic.com/~/media/products/docs/whitepapers/12023-cloud-computing-wp.pdf

[4] http://www.comp.leeds.ac.uk/mscproj/reports/1011/wang.pdf

[5] http://www.bluelock.com/blog/cloud-computing-a-five-layer-model/

[6] http://blogs.computerworld.com/18338/the_three_layers_of_cloud_computing

[7] http://en.wikipedia.org/wiki/Cloud_computing

[8] http://www.itinfo.am/eng/cloud-computing/

[9] Jingwei Huang* and David M Nicol http://www.journalofcloudcomputing.com/content/pdf/2192-113X-2-9.pdf

[10] Ziegler CN, Lausen G (2005) Propagation models for trust and distrust in social networks. Inf Syst Front 7(4–5): 337–358.

[11] http://www.bluelock.com/blog/cloud-computing-a-five-layer-model/

[12] Christian Cachin, Matthias Schunter, http://spectrum.ieee.org/computing/networks/a-cloud-you-can-trust

[13] http://www.ey.com/GL/en/Services/Advisory/Building-trust-in-the-cloud

[14] Khan, K.M. ; Dept. of Computer Sci. & Eng., Qatar Univ., Doha, Qatar ; Malluhi, Q. , http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6576765

[15] Punam Bedi and Hema Banati ,Department of Computer Science, University of Delhi, http://www.di.unipi.it/~cerone/courses/fmais-2010/papers/BB-06-JCS-assessing.pdf

[16] Ms. Heena Kharche ,Mr. Deepak Singh Chouhan Building Trust In Cloud Using Public Key Infrastructure

[17]. Debabrata Nayak, Understanding the Security, Privacy and Trust Challenges of Cloud Computing

[18] Adrienne Hall, Enabling trust in the cloud,

[19] Noman Mazher Imran Ashraf 2A Survey on data