ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.2 , No.6, Pages : 70-73 (2013)
Special Issue of ICETEM 2013 - Held on 29-30 November, 2013 in Sree Visvesvaraya Institute of Technology and Science, Mahabubnagar – 204, AP, India

TEFS, Trust and Cloud Computing

Pranjal Verma[1]
[1]Shanti Business School, India, pranjal.v13@shantibschool.edu.in

Abstract: Cloud Computing is an emerging topic amongst IT personnel. Pay as you go is the basis of cloud computing. It makes data services to be available in enormous speed and with greater ease but the data reside outside the organization's boundaries. Trusting the cloud provider is inevitable. Building Trust is the need of the hour and one organization cannot live without it. We will study the key factors thereby which we will be able to measure and build trust between the cloud provider and the user.

Key words: Cloud Computing, TEFS, Trust, PaaS, SaaS, IaaS.

INTRODUCTION

Cloud computing is a way by which IT needs of an organization can be managed on use basis by the cloud provider.

The cloud itself is a set of hardware, networks, storage, services, and interfaces that enable the delivery of computing as a service. Cloud services include the delivery of software, infrastructure, and storage over the Internet (either as separate components or a complete platform) based on user demand.[1]

Cloud computing services are of several types:

Platform as a Service (PaaS) ensures that the platform is provided for application hosting and running over the cloud.

Another type is Software as a Service (SaaS), in which software or application is provided to the user.

Infrastructure as a Service (IaaS) provides infrastructure to the user to carry out user's business functions.

Pay per use model is used by cloud computing whereby the user only pays for what computing services he uses.

Data center is located remotely. Distributed servers are used, due to which the cloud user doesn't know where the sensitive data resides. All these reasons make cloud user vulnerable to security threats.

WHAT IS TRUST?

Trust is a psychological state that exists when you agree to make yourself vulnerable to another because you have positive expectations about how things are going to turn out.[2]

Cloud user doesn't have complete control of the environment and situation, yet takes risks to use services of the cloud provider. This cloud user makes an assumption that his needs will be fulfilled without compromising with privacy and security.

In terms of cloud computing, the software is hosted at other's disposal (PaaS), or the organization's sensitive data is used on other's software (SaaS), or the complete infrastructure (IaaS) used to carry out IT processes belongs to the cloud provider.

Privacy and security cannot be foolproof. Scope for improving the security of the data will always be there even if encryption is done over the data.

Trust comes into picture to ensure the cloud user is in line and in cordial relationship with the cloud provider.

WHAT IS TEFS?

Trust can be measured using four types of analyses. Cloud user can judge a cloud provider based on:

1) Terms & conditions analysis
2) Experience analysis
3) Feedback analysis
4) Survey analysis

The four analyses can be shortened and named as TEFS.

The cloud user can be expected to analyze any one or all of the above to decide which provider can be taken into consideration and to what extent. Critical data is at stake which makes it important to use any one or all of the above analyses to come to a consensus on which provider is to be chosen.

Rating from one to five can be used to measure the trust level. One refers to highly undesirable, two as undesirable, three as neutral, four as desirable and five as highly desirable.

Averages of individual analysis can be found out if there is more than one parameter to judge the provider. For example, if terms and conditions have two parameters to judge with ratings 3 and 4 each, then average rating would be T-3.5 i.e. 3.5 rating corresponding to Terms & conditions analysis.

Terms & conditions analysis:

Terms and conditions depicted before using the cloud services can help to decide whether the terms of the provider aligns with that of the user or not. Privacy policy can be

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.2 , No.6, Pages : 70-73 (2013)
Special Issue of ICETEM 2013 - Held on 29-30 November, 2013 in Sree Visvesvaraya Institute of Technology and Science, Mahabubnagar – 204, AP, India

brushed up before accepting the conditions of the cloud service provider to check whether the data to be stored over cloud will be safe or not.

Experience analysis:

Current or past experiences with the cloud provider can encourage or discourage using the services further. Trust level can be measured using this type of analysis.

Feedback analysis:

Feedback can be taken from the cloud provider's existing customers. Feedback is a useful tool to measure the trustworthiness of the cloud provider.

Survey analysis:

An inference can be drawn by the surveys, certificates won and the overall ranking of the cloud provider.

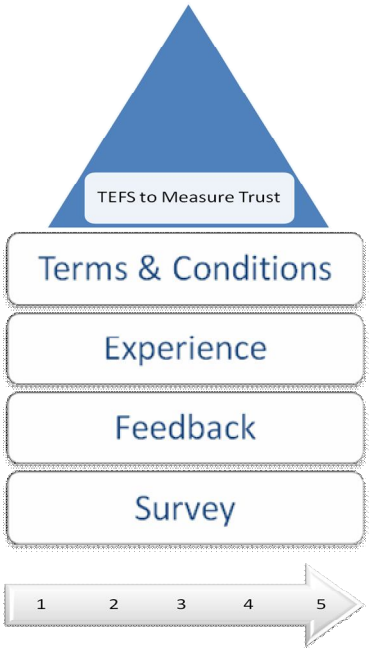

Fig 1: Measuring Trust based on analysis done by the cloud service user

TEFS AND MODEL OF TRUST

As depicted in Fig 2, a popular model of trust by Mayer, Davis, and Schoorman suggests that three major factors determine trust: characteristics of the trustor, characteristics of the trustee, and the perceived risk.[3]

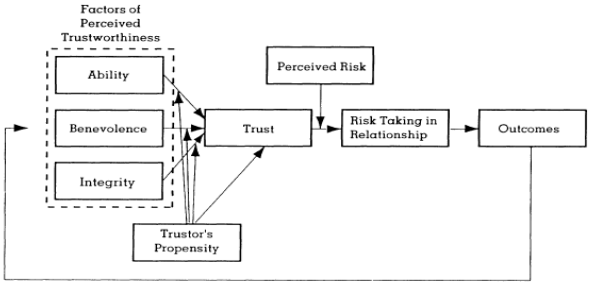

Fig 2: Mayer, Davis, and Schoorman's Model of Trust

This model can be incorporated with TEFS for analyzing trust in cloud computing provider.

Integrity refers to honesty and truthfulness. It seems the most critical characteristic in assessing another's trustworthiness.[4] It also refers to having consistency between what you do and what you say.

Benevolence means the tendency to do well.

Ability is the capacity to do something.

Trust Propensity refers to how likely a particular company is to trust another company.

TEFS will help in analyzing how likely a particular cloud user is to trust a cloud service provider.

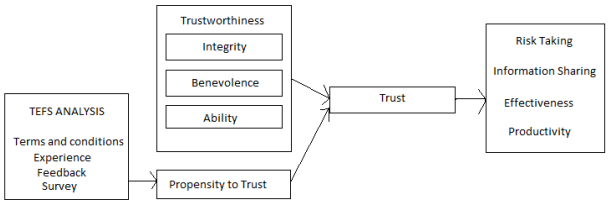

Fig 3: TEFS and Model of Trust for Cloud Computing

OUTCOMES OF CLOUD TRUST

Risks, information sharing, effectiveness and increase in productivity takes place when there is trust between the two parties.[5]

Taking risk is necessary as without risk cloud user will not be able to use the resources of cloud provider efficiently.

Information sharing takes place between the cloud provider and cloud user which is vital for running up the businesses.

Overall effectiveness increases as with trust both the parties are willing to help each other.

Productivity goes high when trust takes place. With increase in cloud user's productivity, cloud provider's productivity increases.

HOW TO BUILD TRUST?

Without trust, neither the cloud provider nor the cloud service user can survive. Trust is the building block for trade to take place between the two.

Trust is a relationship with which both the parties interact with each other and cooperate to work together in the open market.

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.2 , No.6, Pages : 70-73 (2013)
Special Issue of ICETEM 2013 - Held on 29-30 November, 2013 in Sree Visvesvaraya Institute of Technology and Science, Mahabubnagar – 204, AP, India

Ensuring high security procedures adopted by the cloud service provider. High security strengthens the trust and makes IT services less vulnerable to attacks.

Privacy policy followed should be disclosed in the terms and conditions and provider should adhere to it.

Highly reliable services should be given by the provider to ensure trust is maintained. Reliability should not be compromised at any cost as one party is reliable on another party.

Cooperation between the two parties should be there so that the critical data is not leaked out. Mutual cooperation leads to success of both the parties.

Data Mining must be avoided by the provider. Other organization's data should be treated as confidential and not as a tool to sneak into the operations of the cloud user by breaching its confidentiality.

Data encryption should be done by the cloud user to ensure safety of the data. Safeguarding data is necessary to sustain in the globally competitive market.

Data center's physical security should not be compromised. Measures should be taken to isolate the physical presence of the servers.

Transparency should be there between the two parties to promote trust. Useful data should be shared openly and same should be with regarding to monetary issues.

Respect for each other's business objectives and goals should be there. To build trust, it's important to understand each other's goals and work accordingly to achieve them.

Sense of Caring towards each other's organization should be there to ensure trust between them remains for a longer period of time.

Signing MoU (Memorandum of Understanding) expressing a convergence of will between the parties, indicates an intended common line of action.

Signing DPA (Data Processing Agreement) which often contains norms regarding transferring the data to third party.

Frequent Backups by the cloud provider ensures that the data is saved from the unwanted server failures. Prior permission to take backups should be taken from cloud user. This backup feature requires trust that the data is not disclosed to anyone.

Frequently updating server configuration helps increase efficiency of the servers and lowers the downtime. Better the services better the trust between the two parties.

Cloud providers should try to meet SLA's on time to ensure bugs are taken care of at the right time. Dashboards related bugs and problems decline the trust level as down time of server increases.

Full knowledge should be shared by the cloud provider where all the data resides on the distributed server so that cloud user has the complete knowledge about the flow of the data from all the sources.

Payment should be paid on time by the cloud user. Late payments should be avoided as it not only creates distrust but also leads to barriers in the relations of the two parties.

99.99999% ("seven nines") uptime should be aimed by the cloud provider so that it does not affect the business of the cloud user.

Providing cloud services on timely manner without compromising with the quality of the service.

Work ethics should be adhered to when it comes to dealing with relations

Better CRM strategies should be used by cloud provider to maintain relationship with the cloud user.

To decrease dependability, complete data of the organization should not be kept on cloud, instead several cloud providers can be used or only some part of the data should be kept on cloud.

Optimum pricing should be charged to gain the trust of cloud user so that user doesn't feel overcharged and lose trust in the provider.

Reliable and quick services should be provided. Technical support when given on time appreciates the services of the provider and strengthens the trust with the user.

If shared, organizational secrets should not be disclosed at any cost by either of two parties.

Use of copyrights and patents ensures the security of the Intellectual property of the firm.

Intrusion Detection and Prevention Systems [IDS/IPS] should be deployed on cloud servers to report and avoid malicious activity.

The above tactics helps in building trust which is an essential ingredient to sustain in the market in the era of cloud computing.

TEFS Analysis will help in measuring the degree to which trust can be done and with the help of the mentioned tactics, trust can be built.

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.2 , No.6, Pages : 70-73 (2013)
Special Issue of ICETEM 2013 - Held on 29-30 November, 2013 in Sree Visvesvaraya Institute of Technology and Science, Mahabubnagar – 204, AP, India

CONCLUSION

This paper concludes with the fact that the cloud user should analyze the cloud provider on basis of terms and conditions, past experiences or experiences of others, feedback collected about the provider or survey conducted to judge the provider or all of the above. TEFS can be calculated on a scale of 1 to 5, with 1 being highly undesirable to 5 being highly desirable. Cloud trust model was made with defining the TEFS into the existing trust model. Model for building or developing cloud trust can be made as an extension to this paper.

ACKNOWLEDGEMENT

It would be my privilege to thank Prof. Amit Saraswat for creating a vibe in me to write a research paper. I would also like to thank Viral for providing me the links to various research papers.

REFERENCES

[1] Judith Hurwitz, Robin Bloor, Marcia Kaufman, and Fern Halper, *cloud computing for dummies*, Wiley Publishing, Inc., Indianapolis, Indiana, ch.1, pp. 9.

[2] D.M Rousseau, S.B Sitkin, R.S Burt, and C.Camerer, "Not So Different After All: A Cross-Discipline View of Trust", *Academy of Management Review (July 1998)*, pp. 393-404l; and J. A Simpson, "Psychological Foundations of Trust", *Current Directions in Psychological Science 16* no.5 (2007), pp. 264-268

[3] R.C. Mayer, J.H. Davis, and F.D. Schoorman, "An Integrative Model of Organizational Trust," *Academy of Management Review*, Vol. 20, 1995, pp. 709-734.

[4] H.H Tan and C.S.F. Tan, "Toward the Differentiation of Trust in Supervisor and Trust in Organization", *Genetic, Social, and General Psychology Monographs* (May 2000), pp.241-260

[5] Stephen P. Robbins, Timothy A. Judge, and Neharika Vohra, *Organizational behavior*, Pearson Education, Inc., United States, ch 12, pp. 417-419