Calculation of Exploitation Degree at IAAS

Archana B Saxena[#1], Sanjive Saxena[*2]

Associate Professor, Department of Information Technologyr[1#],
Associate Professor, Department of Information TEchnology[2#]
JIMS (Jagan Institute of Management Studies)
3, Institutional area, Sector-5 Rohini, Delhi, India

***Abstract* —** *The rapid growth of cloud computing and its rapid adoption by business units including government organizations has transformed the means and mechanism for doing business. For, as is well known, that cloud offers as easy mechanism for increasing the savings on various aspects of cost such as maintenance costs of various devices and paying only for the services availed from the cloud service provider. However, despite several advantages, the customer on the cloud is at the risk of being exploited either by the business competitors or the cloud service provider may on its own exploit the customer. This paper is an attempt to develop the mathematical model for determining the degree of exploitation due to loss of trust in cloud. The design of the paper follows a structured approach. it starts with the basics of cloud computing and the various assumptions used in the development of the model. It takes into account several practical aspects and finally arriving culminating at the end wherein it highlights the means and mechanism which can be deployed to lessen the impact of the degree of exploitation on account of loss of trust at the IAAS level.*

Keywords - *Cloud, IAAS, Trust, Exploitation, Impact.*

I. INTRODUCTION

The business world of today is slowly but surely adopting cloud as a prime component for managing the business process. This may be due to the fact that business is getting more and more complex as well as competitive in nature. Coupled with this complexity the competitors are struggling to keep the profit margins under control and are thus performing tasks with reduced profit margins. In such a scenario, the cloud offers an optimal medium for carrying out various business processes. For, the cost overheads and other associated maintenance costs of IT infrastructure are borne by the cloud service providers.

However, despite numerous benefits offered by the cloud, of late, there have been incidences wherein the issues related to cloud service providers have surfaced. Primarily the issues relate to loss of trust on the cloud service provider as they have compromised the clients data or other vital information. In other words, the customer's are of the opinion that their data has been compromised. In other words, their has been exploitation of the data by the cloud service provider and the consequent result is the fact that trust has been lost.

While it is difficult to assess loss of trust as well as the degree of exploitation by the cloud service provider at various levels of cloud but nevertheless the authors have tried to develop a mathematical model for determining the same.

Some basic definitions

Before we dwell further, in this paper, it is worthwhile to understand the basic concepts of the various terms as are used in the paper

***Trust*:** For the purpose of this paper, trust is understood as an assurance to the client or the customer regarding some aspect of the service which is being provided by the cloud service provider. Further, this assurance must be on sustained and continued basis for the entire cycle of the contract. Moving further, the assurance must be ardently supported by visible demonstrable indicators. If this is no element of visibility then the assurance will take a nosedive.

Loss of trust: In simple parlance the words loss of trust is construed to mean the failure of the client service provider to provide the same level of trust to the customer. Further, there must be an element of visible or demonstrable indicators and that these indicators must be comparable at different points of the life cycle of the contract. The loss of trust can have the consequences such as cancellation of the contract, dent in the reputation of the cloud service provider and the like

***Cloud*:**In simple terms the word cloud refers to a concept which as three major components. These major components are IAAS, PAAS and the SAAS. These three components are respectively related to Infrastructure, Platform and the Software. The cloud is managed by the cloud service provider who charges the customer according to the consumption pattern. In other words, he provides service to the customers.

Exploitation: In simple terms the word exploitation is referred to as the process of seeking advantage from one entity to another entity. The entities can be competitors, the cloud service providers or it can be the client also.

Degree of exploitation*:* In simple terms the degree of exploitation refers to a number on a certain scale which depicts the level or the depth of the loss which a particular entity has suffered on account of the loss of trust due to another entity.

Having understood the basic definitions let us now move on process of development of the paper. Section II will discuss Reasons for Development of Paper, section III assumptions used in paper, Section IV describe Mathematical Model, Section V lists Limitations of the paper, Section VI Future scope of the paper section VII mention conclusion and Section VIII gives list of references.

II. Reasons for Development of Mathematical Model

The prime reason for the development of the mathematical model for determining the degree of exploitation due to loss of trust is the fact that several research and studies have been conducted on the issues of loss of trust at the cloud. However, as per the existing literature review there has been relatively few studies on the determination of degree of exploitation from practical perspectives. Further, while most of the researcher has focussed on the assessment of the loss of trust in the cloud, the authors of the paper have gone a step further in determining the degree of exploitation. In other words, instead of being confined to the cloud service provider the authors have focussed on other external aspects of the trust.

III. Assumptions used in the paper

The following are the assumptions which have been used in the paper:

A. The existence of the linear relationship among the variables which are responsible for determining the degree of exploitation. This is the basic assumption on which the model is developed.

B. The parameters have been chosen on the basis of their effect on the exploitation aspects.

C. The number of parameters which are responsible for affecting the degree of exploitation may increase or decrease.

D. As the degree of loss of trust can occur at any level of the cloud, for the purpose of this paper the authors have restricted the exploitation level at the IAAS level. The service component being services provided by the cloud service provider at the server level

E. The mathematical model is oriented from the customer's perspective who has availed or is availing the services of the cloud and is thus exploited by several other parameters

IV. Development of Mathematical Model

The following are parameters which have been chosen for determining the degree of exploitation of the client by the services provider

a. Commitment to customer by the client service provider to provide uninterrupted services of the server on 24x7x 365 basis for an enhanced fee of 10% over the existing fee paid by the client.
   a. The scope of the service will include certain minor aspects such as additional server space, unlimited access to the changes on the server and the like
   b. Other scope of the services include the server downtime for half an hour due to maintenance issue
b. Commitment to rectify technical problems at the customer's site on account of which the customer is unable to access the services of the cloud

Thus with these two situations as the base we proceed to develop the paper.

a) Let the enhanced fee paid by the client by $\boldsymbol{\alpha}$
b) Let the time duration for the service provide be denoted by $\boldsymbol{\beta}$
c) Let the extra services *such as increased server space be* denoted by $\boldsymbol{\gamma}$

Thus the customer is presented with the package

$P_1 = (\boldsymbol{\alpha_1, \beta_1, \gamma_1})$ **(i)**

The client service provider already has an old client with the package

$P_2 = (\boldsymbol{\alpha_2, \beta_2, \gamma_2})$ **(ii)**

Where $\boldsymbol{\alpha_2 > \alpha_1}$ i.e. in other words, the old customer is paying greater amount for the same set of variables. [why as is paying]

However, due to increasing business requirements, the old client P_2 needs more server space and the client service provider due to contractual obligations agrees to do so *at the cost of the server allocated to the customer* P_1 as he is not utilizing the allocated server space.

Hence the customer is exploited and the consequent the degree of exploitation can be represented by the following

$DE_{\alpha} = \boldsymbol{\alpha_1 / \alpha_2}$ **(iii)**

where DE_{α} represents the degree of ratio of exploitation with respect to the parameter **α**
In the similar parlance the degree of exploitation can be represented by the equation

$DE_{\beta} = \beta_1 / \beta_2$ **(iv)**

$DE_{\gamma} = \gamma_1 / \gamma_2$ **(v)**

Having got the respective DE's for the various external parameters, we can now use the linear relationship to determine the *degree of exploitation* of the customer.
Hence, we get

$DE = DE_{\alpha} + DE_{\beta} + DE_{\gamma}$ **(vi)**

As equation (iii), (iv) and (v) are ratios, the result would be a ratio. In other words this represents the degree of exploitation of the customer by the client service provider

Interpretation of equation (iv)

DE can have three values.
DE=0 represents that there has been no exploitation by the service provider on the client who is not an old customer. In other words the client service provider is honest in his dealing and has not resorted to any unethical practices
DE <1 or DE>1 represents that the client service provider has resorted to exploitation of the customers due to factors **α, β or γ** and that the anyone of these factors or parameters has had a profound effect on the client service provider

V. LIMITATIONS OF THE PAPER

Although the authors have tried to develop the paper by covering only the macroscopic parameters or factors which provide the impetus for exploitation there can be several other factors which contribute to exploitation process. For example, the inputs for exploitation can be to garner new and potential customers who have more paying capacity. This aspect can be taken up as a scope for further study.

VI. FUTURE SCOPE OF THE PAPER

The model can be modified to include other relationships as is widely applicable in practical scenario. For example, instead of having the linear relationship we can have orthogonal relationship. This will provide further input to the development of the model

VII. CONCLUSION

The paper has provided a new insight to the process of determining the degree of exploitation of trust and further the genesis of exploitation can be a factor which can significantly impact the outcome.

VIII. REFERENCES

[1] .Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy Katz, Andykonwinski, Gunho Lee, David Patterson, Arielrabkin, Ion Stonica and Mateizaharia. "*A View of Cloud Computing*", Communication of the ACM, April 2010, Vol 53, No.4

[2] Ahmed Rashidi Isfahan, Isfahan Iran, "*A Model for Trust in Cloud Computing*", International Journal on Cloud Computing: Services and Architecture (IJCCSA), Vol 2, No.2 April 2012.

[3] Khaled M Kahn and Qutiabah Malluhi, "*Establishing Trust in cloud*", IEEE Computer Science, IT PRO, Sep/Oct 2010

[4] "*Building Trust in the Cloud*", Insights on Governance, Risk and Compliance, June 2014.

[5] William R. Claycomb, "*Cloud Computing Security Turorial*", Carnegie Mellon University, 2012.

[6] Candid Wueest, Mario Balano Barcena, Laura O'Brien, "*Mistakes in the IaaS Cloud can put your Data at Risk*", Security Response, Symantec, Version 1.01, May 2015.

[7] Bijayalaxmi Purohit, Pawan Prakash Singh, "*Data Leakage Analysis on Cloud Computing*", International Journal of Engineering Research and Application, Vol. 3, Issue 3May-June 2013. ISSN: 2248-9622.

[8] Christian Priebe, Divya Muthukumaran, Dan O'Keeffe, David Eyers, Brian Shand, Ruedigerkapitza, Peter Pietzuch.,"*Cloud Safety Net: Detecting Data Leakage between Cloud Tenants*" CCSW'14, November 7, 2014, Scottsdale, Arizona, USA. ACM 978-1-4503-3239-2/14/11.

[9] "*Data Leakage – Threats and Mitigation*", SANS Institute InfoSec Reading Room. Peter Gordon.

[10] http://www.computerworld.com/article/2487123/data-privacy/cloud-computing-2014--moving-to-a-zero-trust-security-model.html.

[11] http://www.washingtonpost.com/business/economy/michaels-says-nearly-3-million-customers-hit-by-data-breach/2014/04/18/3074e432-c6fc-11e3-8b9a-8e0977a24aeb_story.html.

[12] http://www.cloudcomputingexpo.com/node/ / 3204068