www.ijecs.in
International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 5 Issue 10 Oct. 2016, Page No. 18694-18696

Impact of Security Risk on Cloud Computing Adoption

Shashank Mishra[1], Manju. Pandey[2]

[1]DST – CIMS, Banaras Hindu University,
Banaras Hindu University, Varanasi, India -221005
Shashankmishra519@gmail.com

[2] DST – CIMS, Banaras Hindu University,
Banaras Hindu University, Varanasi, India -221005
mpnd@rediffmail.com

Abstract: ***Cloud computing provides application and services over the Web. The services are provided to all over the world by the data centers, which is referred to as the "cloud." This mechanism provides solution to the many network connections and Computer systems in online services. This shows the broad reach of internet, while we are simplifying its complexity. Any user with an Internet connection can use the cloud services provided by it. when these services are connected, users can share information to each other and also to the web. But before entering into the cloud we have know that the rapid growth of cloud computing also increases sever security concern. The Security of cloud is a big issue for open system and cloud computing. It has many security issues like analyzing the data privacy, security auditing and data monitoring. Till now the existing models are too far away to cover the full complexity of the cloud computing model. Some papers has been proposed previously for security of cloud computing but the implementation proposed by them is not enough for full complexity of cloud. In this paper we are going to implement a new mathematical algorithm for low level of risk in Cloud computing environment. The purpose of this attempt is to focus (or provide mechanism) on some new points where the security level founds very low.***

Keywords: Cloud Computing, Security, Data privacy, Hypothesis**.**

1. Introduction

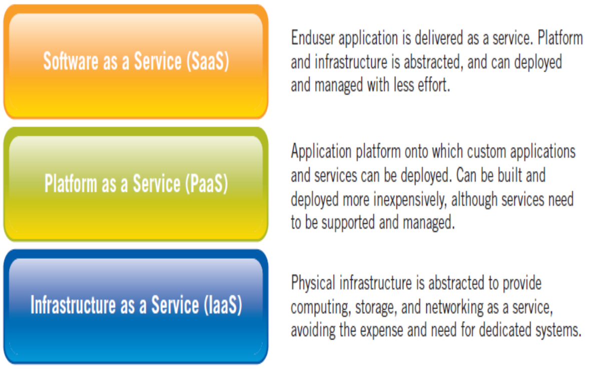
Cloud computing provides the delivery of computing resources over the Web (Internet). Instead of having the data on your systems 's Memory , you can use a service over the Web (Internet), at any location, to store your data or to use of it's application. Cloud computing is providing the computing services over the Web (Internet). Cloud services provides the service to individuals and businesses to use s/w and h/w that are maintained by third parties at any locations. Examples of cloud services is like online file storage, social networking websites, webmails, and online business applications. The cloud computing model allows to use the information's and computer resources from anywhere. Cloud computing gives a shared platform of resources, including Memory space, network, power need for process, and user applications.

This time Cloud computing is one of the biggest technologies around us. Companies are providing billions of dollars applications and data centers to the cloud services. But in a way to move into cloud services , many companies have neglected to confirm that cloud security is made into their models. Firms often assume that a cloud vendor is a secure cloud vendor. Nothing could be further from the truth. Not all cloud vendors are created equal and the levels of security and privacy protection they provide ranges from world class to world's worst.After the creation of cloud, distribution of cloud computing varies with reference to the requirements and for which it will be used. The standard service models being arranged are :-

Software as a Service (SaaS) — Customers purchase the skill to contact and use an application or service that is presented in the cloud. Benchmark sample of this is Salesforce.com, as discussed before, where essential information for the communication between the customer and the service is presented as portion of the service in the cloud.

Platform as a Service (PaaS) — Customers purchase contact to the stages, enabling them to organize their own software and applications in the cloud. The OS and network access are not achieved by the customer, and there might be restraints as to which applications can be organized.

Infrastructure as a Service (IaaS) — Customers control and achieve the systems in terms of the operating systems, applications, Memory, and network connectivity, but do not themselves switch the cloud infrastructure.


Software as a Service (SaaS)
Platform as a Service (PaaS)
Infrastructure as a Service (IaaS)

Enduser application is delivered as a service. Platform and infrastructure is abstracted, and can deployed and managed with less effort.

Application platform onto which custom applications and services can be deployed. Can be built and deployed more inexpensively, although services need to be supported and managed.

Physical infrastructure is abstracted to provide computing, storage, and networking as a service, avoiding the expense and need for dedicated systems.

2. Objective :

The main aim of this attempt is to provide a secure mechanism for security of cloud computing adoption. It will be applicable where the security of cloud computing found to be very less.

3. Deployment Models :-

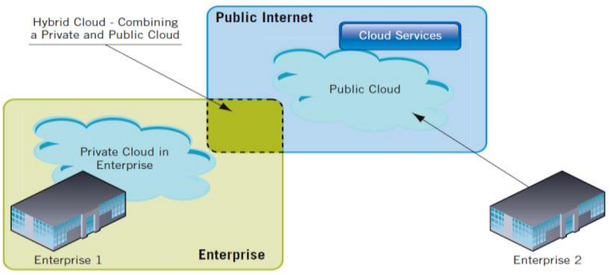
Organizing cloud computing can vary depending on supplies, and the following four deployment models have been known, each with precise characteristics that support the essentials of the services and users of the clouds in specific ways.

Private Cloud — The cloud infrastructure has been organized, and is preserved and functioned for a specific association. The operation may be in-house or through a third party on the buildings.

Community Cloud — The cloud infrastructure is mutual among a number of administrations with similar interests and necessities. This may help limit the capital spending costs for its creation as the costs are shared among the administrations. The process may be in-house or with a third party on the buildings.

Public Cloud — The cloud infrastructure is offered to the public on a marketable basis by a cloud service provider. This allows a customer to develop and organize a service in the cloud with very little economic outlay compared to the capital spending supplies normally related with other placement options.

Hybrid Cloud — The cloud infrastructure contains of a number of clouds of any kind, but the clouds have the ability through their boundaries to allow data and/or applications to be relocated from one cloud to another. This can be a combination of private and public clouds that support the condition to recall some data in an organization, and also the need to suggest services in the cloud.


Hybrid Cloud - Combining a Private and Public Cloud
Public Internet
Cloud Services
Public Cloud
Private Cloud in Enterprise
Enterprise 1
Enterprise
Enterprise 2

4. Literature Review :

Model 1 : In the previous existed model [4] [5] they have focused on ideal adoption rule in which if the adoption grants indeterminate project value as well as the strength of safety risks.

Model Process : In that process they have assumed that the value from the cloud computing implementation has been considered by a wall process.

$$\boldsymbol{dX(t) = \alpha X(t)dt + \sigma X(t)dW_1(t) - X(t)dL_1(t),}$$
$$\boldsymbol{X(0) = x}$$

$$\boldsymbol{dL_1(t)_{(\lambda_1 \cdot \phi_1)} = \begin{cases} \phi_1, & \textit{with probability } \lambda_1 dt \\ 0\,, & \textit{with probability } 1 - \lambda_1 dt_1 \end{cases}}$$

Model 2: The Ideal exchange of two risky resources Model is proposed to achieve the ability of ideal shifting from one to another computing sample, where we need to identify the value related with these two different computing paradigm.

1) **Source of Prospective profits for Cloud Computing Vs On-site Computing**.
-Better Optimization of Operational Expense
-Better optimization of Capital Investments
-Better Speed and Flexibility of Executing Commercial Changes
-Better Attentiveness on Reaching Commercial Objectives
-Better Scalability
-Lower Cost/Risk/Time in Initial a New Commercial Model
-Lower Entry Barriers
2) **Process for Possible Profits of**
-Cloud Computing deployment
-Outmoded On-Site Computing Disposition

5. Approach :-

We are implementing a new algorithm based on the Hypothesis testing and trying to point out the minor time spaces from where the leakage of security might be possible. In the previous papers[1],[2],[3] they have focused on some common points of cloud computing where security is always necessary. With a combination of mathematical hypothesis testing we can test the leakage of security via the time difference.

6. Model Process :-

The following data were obtained in an experiment designed to check whether there is a systematic difference in the Time obtained with two different scales:

Thread	**Time in Seconds**		
	(x_i) on Scale *I*	**(y_i) on Scale *II***	$D_i = x_i - y_i$
1	0.60	0.57	0.03
2	0.57	0.55	0.02
3	0.55	0.54	0.01
4	0.54	0.51	0.03
5	0.51	0.50	0.01
6	0.50	0.46	0.04
7	0.46	0.45	0.01
8	0.45	0.42	0.03
9	0.42	0.39	0.03
10	0.39	0.38	0.01

Use the matched pairs t – test at 5% level of significance, to test whether the difference of the means of the 'time' obtained with the two scales is significant.

DOI: 10.18535/ijecs/v5i10.59

Let μ_d be the mean of the Time of differences d of the time obtained with two different scales. Then

Null hypothesis H_0**:** $\mu_d = 0$

Alternative H_1 **against** $H_0 : \mu_D \neq 0$ (Two – tailed)

The test statistic under H_0: Since the number of paired observations is small (n < 20), we use t – distribution $t = \dfrac{\overline{D}}{s/\sqrt{n}}$, with $\nu = n-1$ *df*, where $\overline{D}$ and S are the mean and the standard deviation of the sample of the differences $D_i = x_i - y_i$, $i = 1, 2, \ldots, n$.

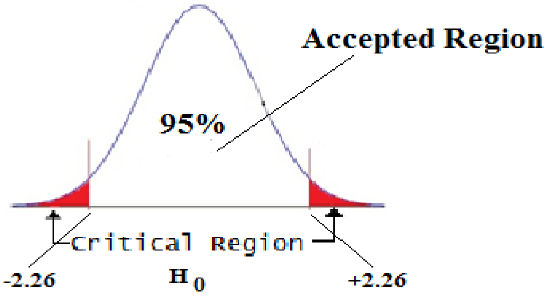
Level of significance: $\alpha = 0.05$

Critical values: With the two – tailed alternative, the 5% critical values of the *t* are $\pm t_{0.05}(\nu = 9)$ = ± 2.26 .

Decision rule: We reject H_0 if $|t| > 2.26$.

Computations: The sample differences of the Time are

0.03, 0.02, 0.01, 0.03, 0.01, 0.04 , 0.01, 0.03, 0.03, 0.01



Then we have $\overline{D} = \dfrac{1}{n}\sum D_i$ = 0.022

$$s = \sqrt{\frac{1}{n-1}\sum (D_i - \overline{D})^2} = .\ 0.02867$$

$$\Rightarrow t = \frac{0.033}{.02867/\sqrt{10}} = 2.206$$

7. Conclusion:

Since the test statistic does not exceed the critical value in magnitude, we do not reject H_0. In other words, it is likely that there is a systematic difference in the Time obtained with two different scales.

References

[1] Mohemed Almorsy, John Grundy and Amani S. Ibrahim. “Collaboration-Based Cloud Computing Security Management Framework” IEEE 4TH International Conference on Cloud Computing, 2011.

[2] Xiang Tana, Bo Aib. “The Issues of Cloud Computing Security in High-speed Railway” International Conference on Mechanical Engineering & Electronic and Information Technology, 2011.

[3] Engr: Farhan Bashir Shaikh and Sajjad Haider. “ Security Threats in Cloud Computing” 6th International Conference on Internet Technology and Secured Transactions, 11 to 14 December 2011, Abu Dhabi, United Arab Emirates.

[4] Wentao Liu. “Research on Cloud Computing Security Problem and Strategy” IEEE 2012. By Hubei Province, China.

[5] Murat kantarcioglu, Alain Bensoussan and SingRu(Celine) Hoe. “Impact of Security Risks on Cloud Computing Adoption” 49th Annual Allerton Conference, Allerton House, UIUC, USA, September 2011.

[6] Yizhang Guan, Jianghong Bao. “A CP Intrusion Detection Strategy on Cloud Computing”. 2009 International Symposium on Web Information Systems and Applications.

Author Profile

Shashank Mishra received the **B.Sc.** in **Mathematics & Physics** from **Bundelkhand University, Jhansi, India** and **M.Sc**. degrees in **Software Technology** from **Vellore Institute of Technology, Vellore, India in 2011 and 2013**, respectively. Currently He is working in a Govt. of India sponsored project at **DST-CIMS, Banaras Hindu University, Varanasi, India – 221005** under the guidance of Prof. Manju Pandey and Prof. Umesh Singh.

Prof. Manju Pandey, is Ex HoD of Computer Science Department, Banaras Hindu University, Varanasi. Currently , She is a Member and also the Principal Investigator of DST sponsored project running at DST – CIMS, Banaras Hindu University, Varanasi, India