ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Study of Security Concern & Challenges in Cloud Computing

Vibha Sahu[1], Praveen Kumar Shrivastav[2], Dipti Chhatri[3], Dr. S.M. Ghosh[4]
[1,2,3]PHD Scholar, [4]Asso.Prof. [1,2]Dr. C.V. Raman University, Bilaspur, India
[3,4] Rungta College Of Engineering & Technology, Bhilai, C.G., India

Abstract: ***The latest developments of information technology offered the people enjoyment and convenience. Cloud computing is one of the latest developments in the IT industry that's give people full comforts and it also known as on-demand computing. It provides the full scalability, reliability, high performance and flexible computing infrastructures. It is the application provided in the form of service over the internet and system hardware in the data centers that gives these services. This technology has the ability to admittance a common collection of resources on request. It is proving extremely striking to cash-strapped IT departments that are wanted to deliver better services under pressure. Cloud has some types when this cloud is made available for the general customer on pay per use basis, then it is called public cloud and it is totally managed by cloud service provider. When customer develops their own applications and run their own internal infrastructure then is called private cloud and there is a contractual agreement between organization and cloud service provider, combination and consolidation of public and private cloud is called hybrid cloud. But having many advantages for IT organizations cloud has some issues that must be consider during its deployment. The major concern is security, privacy and trust . These issues are arises during the deployment of mostly public cloud because in public cloud infrastructure customer is not aware where the data store & how over the internet. Security privacy & trust issues of cloud computing are reviewed in this paper. The paper includes some surveys conducted by IDC and that show the motivation for the adoption of cloud computing. The paper also identifies the issues and the solution to overcome these problems.***
Keywords: ***Cloud Computing, On-Demand computing, Security Issues.***

I. INTRODUCTION

Cloud computing is a Internet-based computing, and it is most recent trend in IT world. In cloud computing shared information resources and software, and that are provided to computers and other devices on-demand. This technology has the capacity to admittance a common collection of resources on request. It is proving extremely striking to cash-strapped IT departments that are wanted to deliver better services under pressure. Concept of this new trend started from 1960 used by telecommunication companies until 1990 offered point to point data circuits and then offered virtual private networks. But due to network traffic and make network bandwidth more efficient introduced cloud to both infrastructure and servers. The development of this Amazon played vital role by making modern data centers. In 2007 IBM, google and many remarkable universities and companies adopted it. In 2008 Gartner highlighted its characteristics for customer as well service providers. This paper provides the guiding principle and considerations required to IT enterprises for the adoption of cloud computing technology and also the awareness of cloud computing power to the IT industry by addressing the global challenges. The paper collect information and statistics surveys conducted by the most popular and standard organizations; like International Data Corporation (IDC) and a brief review of cloud computing security, trust & privacy issues.

II. LITERATURE REVIEW

The literature identifies different broad service models for cloud computing:

A. Software as a Service (SaaS)

where applications are hosted and delivered online via a web browser offering traditional desktop functionality for example Google Docs & MySAP.

B. Platform as a Service (PaaS)

where the cloud provides the software platform for systems (as opposed to just software), the best example being the Google App Engine.

C. Infrastructure as a Service (IaaS),

where a set of virtualized computing resources, such as storage and computing capacity, are hosted in the cloud customers

deploy and run their own software stacks to obtain services. Current examples are Amazon Elastic Compute Cloud (EC2), Simple Storage Service (S3).

III. SURVEY CONDUCTED ON CLOUD COMPUTING BY IDC

This paper covers survey conducted by international data corporation (IDC). It shows the strong point or strength of cloud computing to be implemented in IT industry and gives the potential inspiration to CSP. The survey related to the growth of cloud, security aspect. Cloud is the first priority to the vendors, revenue report, future and current usage, state of cloud to the IT users and popularity survey of cloud computing.

A. Cloud growth

The Table 1 shows the cloud growth from year 2008 to 2012.

B. Survey on cloud security

The Fig. 1 shows the survey on security. This represents security as first rank according to IT executives. This information is collected from 263 IT professional by asking different question related to the cloud and many of the executives are worried about security perspective of cloud.

Table 1 **Cloud Growth**

YEAR	2008	2012	GROWTH
Cloud IT Spending	$ 16 B	$ 42 B	27%
Total IT spending	$383 B	$494 B	7%
Total-cloud spend	$367 B	$452 B	4%
Cloud Total spend	4%	9%	

C. Top ten technology priorities

This report displayed in Fig 2 collected at the end of 2010 by IDC. This shows that now a days the cloud computing is the first priority by organization in the field of technology.

D. World wide IT cloud services revenue by product/service type

The Fig. 3 and Fig. 4 show the survey collected in 2009 by IDC. This survey shows the revenue on cloud in 2009 is 17.4 billion dollars but it will enhance up to 44.2 billion in 2013.

E. Current and future usage of cloud in IT

The Fig. 5 shows the graph that is collected by IDC in August 2009. It shows today's usage and future usage of Cloud in different areas

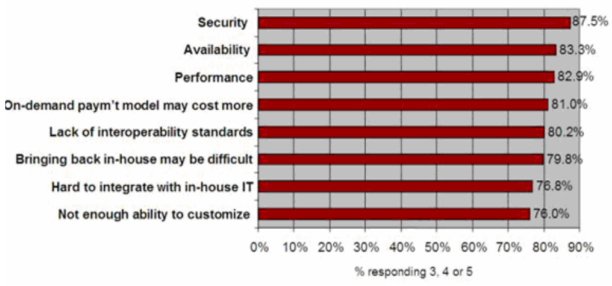

Figure 1: cloud security survey

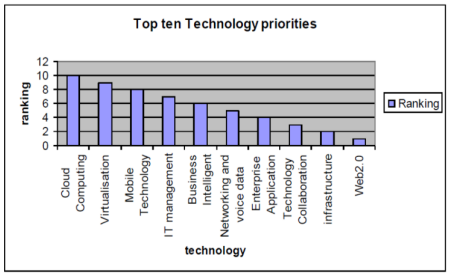

Fig. 2: Top ten technology priorities

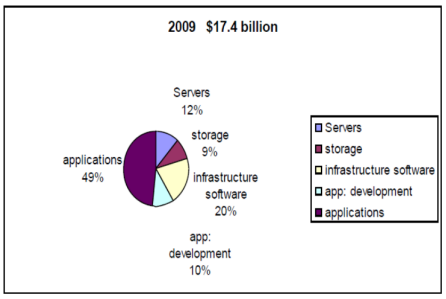

Fig. 3: 2009 revenue report

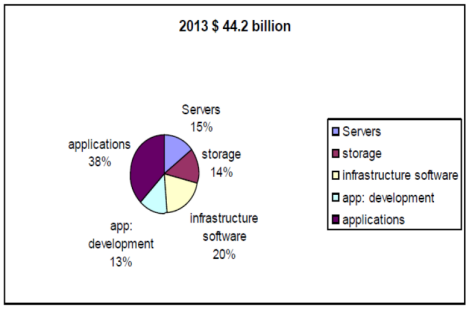

Fig. 4: 2013 expected revenue report

F. Opinion for the state of cloud computing

The chart shows in Fig. 6 show the position of cloud according to different executives. Survey conducted from 696 IT consultants about the status of the cloud, what is their opinion related to it.

G. Survey on popularity

This survey shows in Table 2 demonstrate the popularity of cloud .It illustrates the rapid growth of cloud application, services and devices.

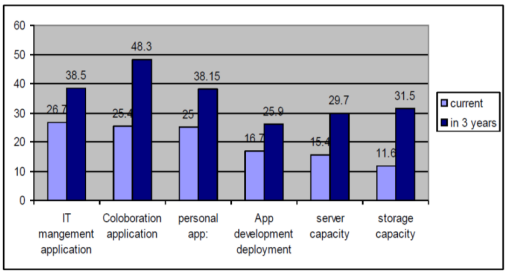

Figure 5: Current & future of cloud usage

Table 2: Increased Popularity

	2010	2011	%GROWTH
Number of Apps	2.3	6.5	82%
Number of Devices	2	4	100%
Connecting Apps to the Cloud	64%	87%	38%

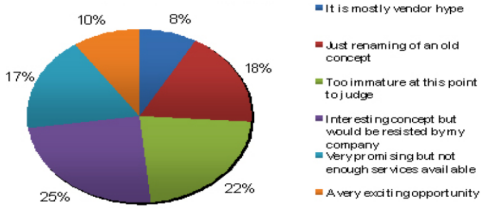

Figure 6: State of cloud computing

IV. CLOUD SECURITY ISSUES AND CHALLENGES

Cloud computing is up-and-coming technology with shared resources, lower cost and rely on pay per use according to the user demand. Due to much uniqueness it has effect on IT budget and also impact on security, privacy and security issues. Here all these issues are discussed. A CSP should give full attention to security aspect of cloud because it is a shared pool of resources. Customer not know where the data are stored, who manage data and other vulnerabilities that can occur. Following are some issues that can be faced by CSP while implementing cloud services.

A. Privacy Issue

It is the human right to secure his confidential and sensitive information. In cloud context privacy occur according to the cloud deployment model. In Public cloud (accessed through the Internet and shared amongst different consumers) is one of the

dominant architecture when cost reduction is concerned, but relying on a CSP to manage and hold customer information raises many privacy concerns and are discussed under.

1) *Lack of user control:* In SAAS environment service provider is responsible to control data. Now how customer can retain its control on data when information is processed or stored. It is legal requirement of him and also to make trust between customer and vendor. In this new paradigm user sensitive information and data is processed in 'the cloud' on systems having no any, therefore they have danger of misuse, theft or illegal resale. Adding more, this is not patent that it will be possible for a CSP to guarantee that a data subject can get access to all his/her PII, or to comply with a request for deletion of all his/her data. This can be difficult to get data back from the cloud, and avoid vendor lock-in.
2) *Unauthorized Secondary Usage:* One of the threats can occur if information is placed for illegal uses. Cloud computing standard business model tells that the service provider can achieve profits from authorized secondary uses of users' data, mostly the targeting of commercials . Now a days there are no technological barriers for secondary uses. In addition, it has the connected issue of financial flexibility of the CSPs: for example, possibility of vendor termination, and if cloud computing provider is bankrupted or another company get data then what would happen.
3) *Transborder Data Flow and Data Proliferation:* One of the attribute of cloud is Data proliferation and which involves several companies and is not controlled and managed by the data owners. Vendor guarantee to the ease of use by copy data in several datacenters. This is very difficult to ensure that duplicate of the data or its backups are not stored or processed in a certain authority, all these copies of data are deleted if such a request is made. Due to movement of data, CP exacerbate the transborder data flow matter because it can be tremendously difficult to ascertain which specific server or storage device will be used, as the dynamic nature of this technology.
4) *Dynamic provision:* Cloud has vibrant nature so there is no clear aspect that which one is legally responsible to ensure privacy of sensitive data put by customer on cloud.

B. Security

Public cloud not only increases the privacy issue but also security concern. Some security concerns are described below:

1) *Access:* It has the threat of access sensitive information. The risk of data theft from machine has more chances in cloud environment data stored in cloud a long time duration any hacker can access this data.
2) *Control over data lifecycle:* To ensure the customer that it has control over data, if it remove or delete data vendor cannot regain this data. In cloud IAAS and PAAS models virtual machine are used that process and then media wiped but still there is no surety that next user cannot get that data.
3) *Availability and backup***:** There is no any surety of availability and back up of data in this environment. In business backup is one of the important consideration.
4) *Multi-tenancy:* It is feature of SAAS that one program can run to multiple machines. CSP use multi-tenant application of cloud to reduce cost by using virtual machine but it increase more vulnerability.
5) *Audit:* To implement internal monitoring control CSP need external audit mechanism .But still cloud fails to provide auditing of the transaction without effecting integrity.

C. Trust

Trust is very necessary aspect in business. Still cloud is fail to make trust between customer and provider. So the vendor uses this marvelous application should make trust. Weak trust relationship and lack of customer trust cause many problems during deployment of cloud services.

D. Mitigation Steps

This section includes mitigation steps and some solution to overcome the issues discussed in previous section. It provides guidelines to the companies that offer cloud services .It will helpful to them to make proper strategy before implementing cloud services. There are some alleviations to reduce the effect of security, trust and privacy issue in cloud environment. There are many adoption issues like user get privilege to control data cause low transaction performance, companies are worried from cyber crimes and as India is now going to developed so the Internet speed also effect the performance, virtual machines are taking milliseconds to encrypt data which is not sufficient and to avoid risk there is contract between parties to access data. So mitigate such type of problems some action should taken place. Some steps are listed below:

1) Build up an iterative policy for relocation from traditional environment to Cloud environment.Vendors in india should follow proper plan moving from their existing system to this new evolution.
2) As this upcoming trend reduce cost but be careful to select possible solutions to avoid problems in this computing and calculate the effect on the system just not consider the outlay.

3) Providers should be aware regarding new changes and assure that customers access human rights are limited.
4) Cloud is a shared pool of resource. Discover the linked service providers that wants to connected to particular Cloud service provider to query, which provider has right to use facts and data .
5) System for monitoring should be request for elimination.
6) Service provider should tell customer for managing polices for security beside provider's owned policies, with in the duration of services. Make it sure, that the data being transferred is protected and secured by standard security techniques and managed by appropriate professionals.

V. PROPOSED SOLUTIONS

Below gives a look on the solutions that are helpful to the cloud customer and companies offer services with secure and trusty environment.

A. Data Handling Mechanism
1) Classify the confidential Data
2) Define policies for data destruction
3) Define the geographical region of data.

B. Data Security Mitigation
1) Encrypting personal data
2) Avoid putting sensitive data in cloud

C. Design for Policy
1) Fair information principles are applicable.

D. Standardization
2) CSP should follow standardization in data tracking and handling

E. Accountability
3) For businesses having data lost, leakage or privacy violation is catastrophic
4) Accountability needs in legal and technical.
5) Audit is need in every step to increase trust
6) All CSP make contractual agreements.

F. Mechanism for rising trust
1) Social and technological method to raise trust.
2) Joining individual personal rights, preferences and conditions straightforwardly to uniqueness of data.
3) Devices connected should be under control by CSP.
4) Use intelligent software.

VI. CONCLUSION

Cloud computing is newest development that provides trouble-free access to high performance computing resources and storage infrastructure through web services. Cloud computing delivers the potential for effectiveness, cost savings and improved performance to governments, organizations, private and individual users. It also offers a unique opportunity to developing countries to get closer to developed countries. Developing countries can take the benefits of cloud computing by implementing it in its e-government projects. The paper addresses the issues that can arise during the deployment of cloud services . After identify these problems some steps are explained to mitigate these challenges and solutions to solve the problems.

VII. FUTURE WORK

Cloud computing is the most modern technology so lots of issues are remained to consider. It has many open issues some are technical that includes scalability, elasticity ,data handling mechanism, reliability, license software, ownership, performance, system development and management and non-technical issues like legalistic and economic aspect. Cloud computing still unknown "killer application" will establish so many challenges and solutions must develop to make this technology work in practice. So the research is not stop here much work can be done in future. The model presented in this paper is the initial step and needs more modifications; however it can provide the basis for the deeper research on security deployment of cloud computing for the research community working in the field of Cloud Computing.

REFERENCES

[1] Chang, L, Ti ; Chin L; Chang, A.Y.; Chun J, C;(2010), " Information security issue of enterprises adopting the application of cloud computing", IEEE

2010 Sixth International Conference on Networked Computing and Advanced Information Management (NCM),pp 645, 16-18 Aug.
[2] S. Subashini, and V. Kavitha. (2010) "A survey on security issues in service deliverymodels of cloud computing." *J Network Comput Appl* doi:10.1016/j.jnca.2010.07.006. Jul.,2010.
[3] Cloud Security Alliance (CSA). Available: http://www.cloudsecurityalliance.org [Mar.19,2010]
[4] Muzzammil Sheikh; (2011), "PTCL Launched EVO USB become Wi-Fi Hotspot", The Frontier Star (Northwest Frontier Province, Jan 26 2011 Issue.
[5] Kresimir P; Zeljko H; (2010), "Cloud computing security issues and challenges", MIPRO 2010, May 24-28, 2010, Opatija, Croatia.
[6] S. Arnold (2009, Jul.). "Cloud computing and the issue of privacy." *KM World*, pp14-22.Available: www.kmworld.com [Aug. 19, 2009].
[7] Tian L.Q; NI Y,LING; (2010) , "Evolution of user Behavior Trust in Cloud Computing", 2010 International Conference on Computer Application and System Modeling (ICCASM 2010),Vol. 7,pp V7-567, 22-24 Oct. 2010.
[8] Mathur, P; Nishchal, N.; (2010), "Cloud Computing: New challenge to the entire computer industry", 2010 1st International Conference on Parallel, Distributed and Grid Computing (PDGC - 2010), pp 223.
[9] Yuefa D; Wu B; Yaqiang G; Zhang Q; Tang C; (2009), " Data Security Model for Cloud Computing", Proceedings of the 2009 International Workshop on Information security and Applications (IWISA 2009) .
[10] Lazowska, E., Lee, P., Elliott, C. & Smarr, L.(2008). "Infrastructure for Escience and Elearning in Higher Education," Computing Community Consortium. [Online], [Retrieve October 5, 2010],http://www.cra.org/ccc/docs/init/Infrastructure.pdf.
[11] Dean and S. Ghemawat; (2010), "MapRduce: Simplified data processing large clusters", communication of the ACM, Vol.51, pages 107-113.
[12] Xue J; Zhang J.J; (2010),"A Brief Survey on the Security Model of Cloud Computing",2010 Ninth International Symposium on Distributed Computing and Applications to Business, Engineering and Science.
[13] Open Security Architecture http://www.opensecurityarchitecture.org.
[14] Tim Mather, Subra Kumaraswamy, Shahed Latif Cloud Security and Privacy : An Enterprise perspective of Risks.