A Review about Cloud Computing Security: Issues and Challenges

R.Lalitha [1],M.Sowmiya[2], P.S.Seemma[3]
Department of Computer Technology
Sri Krishna Arts & Science College, Coimbatore

Abstract: Cloud computing is next generation networkingthat change the world into the computing one. Because of its scalability, performance, security and integrity, it becomes more demand. Nowadays the cloud is growing rapidly in the IT industry and also lot of companies are realizing they can strongly boost their infrastructure, fast accessing to their business by simply utilizing the cloud at negligible cost. So for this advantage the more number of resources have been stored in the cloud and concerns have been started to grow about the safeness about cloud because the services are often shared to the third party, and it became harder to maintain the data security and its privacy. Inthis paper we mainly pinpointed the challenges and issues of cloud computing.

KEYWORDS:cloud computing, cloud security.

INTRODUCTION:

As of today most of the enterprises are using Cloud to expand their infrastructure but most of them were having doubt about the security about their data which is stored in thecloud. So most of them questioned that what is Cloud Computing? It is safe to use or not?To answering these questions we discuss about cloud computing overview, cloud security and its issues and challenges. Mostly the cloud computing is concerned with online software applications, data storage and cloud is a way to increase the capacityof the applications without investing on other new infrastructure or licencing new software but the security issues are playing a major role in the cloud and it slowdownsthe acceptance of cloud to the customer. For this a survey has been conducted by IDC [1] (Fig.1.)From 263 IT executives to get their opinions about the IT cloud services and Corporation are concerned about the security and compliance are being maintained in this new environment. A cloud solution provider will ensure that the customers can continue to have the same security and privacy controls over their applications and it provide an evidence to the customers that their organization and customers are secured.

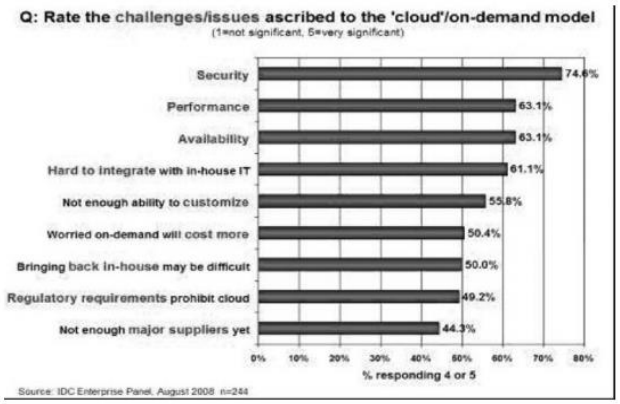

FIGURE 1:survey results of IDC ranking security challenges, 2008

CLOUD SECURITY PILLERS:

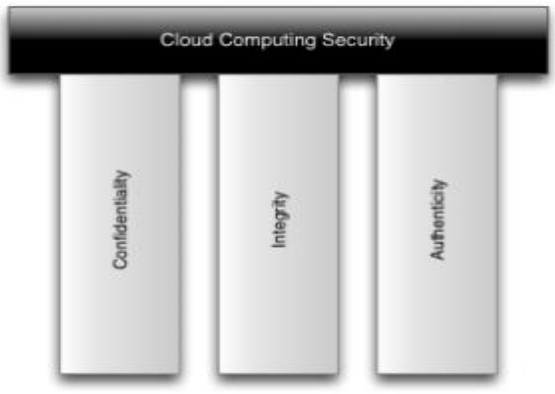

FIGURE 4: cloud security pillars

The types of security pillars in cloud computing are:

A. Confidentiality

Confidentiality of a system should guarantee the users to prevent from unauthorized user. In data secure

systems requires authorizations and to ensure that information cannot be accessed by unauthorized user and this comprises both access to stored data and transfer the data through an network which is authorized by users[2]. Cryptographic techniques and access controls are normally used to protect confidentiality based on strong authentication.

B. Integrity

Data, information and messages are considered to have integrity if they are trustworthy and cannot be meddle with. A system should assure the integrity of the secured dataand the information cannot be modified by third parties. Data must be protected against unauthorized access which is stored on a virtual hard drive for instance.

C. Authenticity

The authenticity of an object is defined as its credibility and these can be verified on the basis of its unique characteristic features. Ifthe Information is authentic and it can be accurately assigned to the sender if it is proved that these informationare not been changed since it was created. A secure technique for identifying the communication partners is essential here. Thiskindof mechanism must be capable of confirming or rejecting of the protected informationauthenticity. Digital signaturesand passwords are enables the signatory of a message to be identified in a cloud computing system.

CLOUDCOMPUTING CHALLENGES:

Themajor challenges that prevent Cloud Computing from being adopted are as follows:

A. Security

The security issue has played the most important role in inhibit Cloud computing acceptance. Without doubtrunning your software on someone else's hard disk by using someone else's CPU appears intimidating to many. Well-known security issues such as phishing, botnet and data loss cause serious threats to organization's data and the pooled computing resources in cloud computing has launched new security challenges that require novel techniques to handle with. For example, hackers will use Cloud to organize botnet as Cloud often provides more reliable infrastructure services at a cheaper rate. [4]

B. Costing Model

The trade-offs amongst computation, integration and communication are must be consider by Cloud consumers and While drifting to the Cloud can importantly reduce the infrastructure rate, then it will raise the rateof thedata communication, i.e. the cost per unit of computing resource used is likely to be increased. This problem is particularly notable if the consumer uses the hybrid cloud wherethe data's of organisation is distributed amongst a number of public/private /community clouds. [4]

C. Charging Model

The cost analysis is lot more complicated than regular data centres which is made by elastic resource and also often calculates their rate based on utilization of static computing, the unit of cost analysis rather than the underlying physical server are instantiated by virtual machine. For SaaS providers, the cost of developing multitenancy within their hand-out can be very considerable. These include: redevelopment of the software used for single-tenancy, cost of producing new features that allow for intensive customization, and user access security enhancement, SaaS providers need to weigh up the trade-off between the cost-savings and the provision of multitenancy such as reduced through reduced number of on-site software licenses, etc. [4]

D. Service Level Agreement (SLA)

Even though the cloud consumers do not have control over the computing resources, they should

need to ensure the availability, reliability, quality and performance of these resources when the business functions are migrated onto their entrusted by cloud consumers. And these are provided through Service Level Agreements negotiated between the providers and consumers. The very first issue is the definition of Service Level Agreements in such a way that has an appropriate level of granularity, namely the trade-offs between complicatedness and expressiveness so that they can cover most of the consumer expectations simple to be verified, evaluated, and enforced by the Kuyoro S. O., Ibikunle F. & Awodele O. IJCN, of Volume (3) andIssue (5) of 2011 253 is the resource allocation mechanism on the cloud. And it also raises a number of implementation problems for the cloud providers. [5]

ISSUES IN CLOUD COMPUTING:

Issues of cloud computing canreviewas follows:

A. Privacy Cloud

The virtual computing technologyis utilized by Computing, users' personal data's aresmattered in various virtual data centre's rather than placed in the same physical location, while accessing cloud computing services, users may leak hidden information . Attackers will able to analyse the critical task which is submitted by the users. [6]

B. Reliability

Thedowntimes and slowdowns are also experienced by the cloud servers like as our local server.

C. Compliance

Numerous acts are involved to the storage and data use and it also requires regular reporting and trails. The data centres' are maintained by the cloud providers it may also concern to compliance requirements.

D. Freedom

The users are allowed by cloud computing to physically possess the storage of data, control the data and leaving the data storage.

E. Long- Term Viability

The user should be sure about the data placed in the cloud ,and that data will never become unavailable even if the cloud computing provider go broke or swallowed by a bigger company.

F. Issues in Cloud Interoperability:

1) Intermediary Layer

The interoperability issue was addressed by a number of recent works by providing an intermediary layer between the cloud-specific resources and the cloud consumers (e.g. VM)[12].

2) Open Standard Standardization

A good solution to address the interoperability issue. The cloud computing take off, the cloud interoperability problem has not been appeared on the pressing agenda of cloud vendors of larger industry.

3) Open API

Under the Creative Commons license the SUN has recently launched the Sun Open Cloud Platform [7]. A major contribution for this platform is the cloud API and it defines a set of clear Restful Web services ,through which are able to create and manage cloud resources by cloud consumers.

4) SaaS and PaaS Interoperability

A group of experts of the field data mining established the issue of data mining standard on the cloud, with focus on "the practical uses of the statistical algorithms, deployment models and the integration of predictive analytics"based on data mining of SaaS cloud. AndPaaS interoperability not yet discovered because it is more difficult to reach the uniformity with consumers develop and deploy cloud applications.

DATA SECURITY AND PRIVACY PROTECTIONISSUES:

Data security and privacy protection contents in cloud are similar to the data security and privacy protection and It is involved in every stage of the life cycle of data. And becauseof the openness of the cloud, the content of data security and privacy protection in cloud storage has itsown particularities. The definition of privacy is adopted by OECD [8] is "any data relating to aprivacy identified individual (data subject)." And Generally speaking, privacy is associated with the collection, storage, and destruction of personal user data. The Identification of private information depends on the specific scenario and the rule, and is the primary task of privacy protection. The issues of the privacy protection are.

A. Data Life Cycle

The entire process from generation to destruction of the data is referred by data lifecycle.And there is seven phases in lifecycle.It is mentioned in below figure 4.

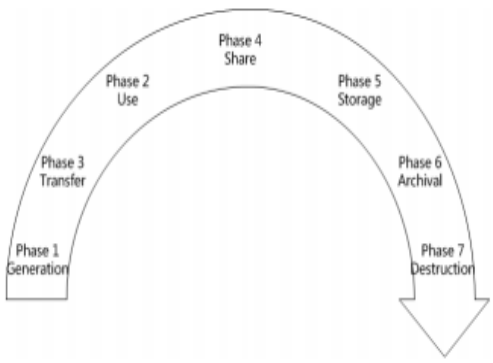

FIGURE 4:phases of data life cycle

B. Data Generation

The data ownership is involved by the Data generation. The users orthe organizations are owns and manage the data it is the usual traditional IT environment, But if data is to be placed into the cloud, then the user started to considered about how to maintain the data ownership.

C. Transfer

Data transmission usually does not require encryption, or not have a simple data encryption measure within the enterprise boundaries. Both data confidentiality and integrity should be ensured in order to prevent data from being tapped with by unauthorized usersfor data transmission across enterprise boundaries. So it should ensure that both confidentiality and integrity are provided by the transport protocols.Confidentiality and integrity should ensure the entire transfer process of data.

D. Share

The use range of the data and renders data are expanded by data sharing and its data permissions are more complex. the data access to one party, which is authorized by the data owners and in turn the party can share the data to another party without the permission of the data owners during the data sharing and especially when the data is shared with a third party.

The data owners always need to consider whether the third party maintaining the original protection measures. And Isolating the sensitive information from the original data are should be referred by the data transformation.This process makes the data is not relevant with the data owners.

E. Storage

The cloud's data are divided into: [9]

(1) Amazon's Simple Storage Serviceis the datain IaaS environment.

(2) Cloud based applications are related to the data in PaaS or SaaS environment.

The data stored in the cloud storagessimilarly the same data saved in other places should consider these 3 aspects of information security they are: confidentiality, availability and integrity.Data encryption is the solution for data confidentiality [11]. In order to make sure the effective of encryption needs to consider both encryption algorithm and key strength usages. As the cloud

computing environment involving large amounts of information transmission, storage, also needs to consider the computational 649 efficiency of encrypting large amounts of data and processing speed. For this casethe symmetric encryption algorithm is more useful than the asymmetric encryption algorithm. Key management is the key problem about data encryption. Is about the who is responsible for thekey management? Actually, it is the data owners. But now, the users are not enough experts in to manage the keys, because they actually entrust the cloud providers from the key management. Key management will become more complex and difficult because the cloud providers need to maintain keys for a large number of users.

The data confidentiality needs to consider about the data integrity. When the users put several amount ofdata (GB or more) into the cloud storage, then the user how to check the integrity of the data?[13]Cloud computing feature of elasticity resources, the users don't know the place of their data is being stored. To migrate out of data into the cloud storage will consume the user's network bandwidth and an amount of time. Such as Amazon like cloud providers, will requires the users to pay transfer fees. Download the data and then upload the data inside the cloud storage is a great challenge. Because the data is dynamic in cloud storage, and the data integrity may not be effective. The main threat of the data availability comes from external attacks is the traditional IT environment. In the cloud, there are several other areas that will threat the availability of the data:[10]

(1) Cloud computing services availability;

(2) In the future whether the cloud providers would continue to operate?

F. Archival

Data focuses on the storage media for Archiving, whether to provide off-site storage duration. The media is out of control if the data is stored on portable mediaand the data are likely to take the risk of leakage [11].The availability of the data will be threatened if the cloud service providers do not provide off-site archiving, and again whether storage duration is consistent with the requirements of archival? If not, this may result in the privacy threats.

G. Destruction

When the data is no longer needed, it is possible to destroy the data completely? But the deleted data may still exist and can be restored by the physical characteristics of storage medium. This may result in unintentionally disclose of sensitive information.

CONCLUSION:

Although cloud computing has many advantages, actually still there are many problems that need to be solved. According to survey about cloud computing revenues by a Gartner, with a compound annual growth rate of 20 market size for Public and Hybrid cloud is $59 billion and it will reach 149B USD by 2014 [14]. Due to the cloud computing is a very promising industry. But from another view, existing vulnerabilities, attacks and unauthorized access in the cloud model will increase the threats. Privacy protection issues and data security are the primary problems that need to be solved as soon as possible.

Sharingthe data while protecting personal information are the challenges in the privacy protection. Example that e-commerce systems that store health care systems with health data. Becomea growing concern for the ability to control the data to berevealed and who can access that information over the Internet.And these concerns include whether personal data's can be stored or read by third parties without consent. According to the analysis for privacy protection and data security issues above, it is expected to have an integrated and comprehensive security solution to meet the needs of defence in depth.

REFERENCES:

[1] International Data Corporation, http://blogs.idc.com/ie/wpcontent/uploads/2009/12/idc_cloud_challenges_2009.jpg, 2009

[2] P. Mell and T. Grance, "Draft nist working definition of cloud computing - v15," 21. Aug 2009, 2009.
[3] M. Armbrust, A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, and I. Stoica, "Above the clouds: A 32 Berkeley view of cloud computing," EECS Department, University of California, Berkeley, Tech. Rep. UCB/EECS-2009-28, 2009.
[4] S. Ramgovind, M. M. Eloff, E. Smith. "The Management of Security in Cloud Computing" In PROC 2010 IEEE International Conference on Cloud Computing 2010.
[5] C. Weinhardt, A. Anandasivam, B. Blau, and J. Stosser."Business Models in the Service World."IT Professional, vol. 11, pp. 28-33, 2009.
[6] J. F. Yang and Z. B. Chen, "Cloud Computing Research and Security Issues," 2010 IEEE International Conference on Computational Intelligence and Software Engineering (CiSE), Wuhan pp. 1-3, DOI= 10-12 Dec. 2010.
[7] "Sun Microsystems Unveils Open Cloud Platform," [Online]. Available: http://www.sun.com/aboutsun/pr/2009-03/sunflash.20090318.2.xml,2 009.
[8] "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data," http://www.oecd.org/document/18/0,3343,en_2649_ 34255_1815186_1_1_1_1, 00.html.
[9] Peter Mell, and Tim Grance, "The NIST Definition of Cloud Computing," Version 15, 10-7-09,http://www.wheresmyserver.co.nz/ storage/media/faq-files/cloud-def-v15.pdf.
[10]Yanpei Chen, Vern Paxson, Randy H. Katz, "What's New About Cloud Computing Security?" Technical Report No.UCB/EECS-2010-5.
http://www.eecs.berkeley.edu/Pubs/TechRpts/2010/EECS-2010-5.html
[11] RandikeGajanayake, Renato Iannella, and Tony Sahama, "Sharing with Care An Information Accountability Perspective," Internet Computing, IEEE, vol. 15, pp. 31-38, July-Aug. 2011.
[12] W. A. Jansen, "Cloud Hooks: Security and Privacy Issues in Cloud Computing," Proceedings of the 44th Hawaii International Conference on System Sciences, 2011.
[13] M. Jensen, J. Schwenk, N. Gruschka and L. L. Iacono, "On Technical Security Issues in Cloud Computing." PROC IEEE ICCC, Bangalore 2009, pp. 109-116.
[14]Gartner DataQuest Forecast on Public Cloud Services DocID G00200833, June 2, 2010.