ISSN: 0975-766X
CODEN: IJPTFI
Available Online through *Review Article*
www.ijptonline.com

A REVIEW ON ISSUES PERTAINING TO CLOUD COMPUTING

Sankeerth Goud A, Grandhi Sampath Kumar
SCOPE, VIT University, Vellore, Tamilnadu, India.
SCOPE, VIT University, Vellore, Tamilnadu, India.
Email: goud.sankeerth@gmail.com

Received on 10-11-2016 *Accepted on: 28-11-2016*

Abstract

Cloud computing has created a rapid change in software paradigm and being relatively new technology but has been adopted widely by many organizations and individual for their computing needs. Definition of Cloud Computing is different from definitions provided by researchers. According to NIST as defined in cloud can be defined as [7] "Cloud computing is a model for enabling ubiquitous, convenient, on-demand Network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models (Software as a Service (SaaS). Platform as a Service (PaaS). Infrastructure as a Service (IaaS) and four deployment models (Private, Community, Public and Hybrid types of cloud)", in this paper we deal with the current issues of cloud, cloud is an evolving rapidly and is latest and most used in software industry. The growing speed of cloud is very fast. The paper gives a quick survey Issues pertaining to cloud computing where customers face when adopting or migrating to cloud.

Keywords: Cloud Computing, Liability, Security Challenges, Service Providers.

I. Introduction

There has been a lot going on in the Cloud Computing Technology domain, IT Experts, Industry leaders and business leaders have been mentioning about cloud in many places. It has been a disruptive technological advancement representing or showcasing the next stage of evolution of the software products and the data domain. So let's see what Cloud Computing actually is?, According to SPECS Open group Systems Group (OSG) - "Cloud computing is a model for enabling ubiquitous, convenient, on demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or provider interaction." we have two different perspectives to define or talk about cloud

they are Users Perspective, Cloud computing provides a means for acquiring computing resources without any pre-defined or trained understating of underlying implementation or idea of the technologies used and from the Organizational perspective, cloud provides services for users and business needs in a simple way where the resources are unbounded, scalable, differentiated quality with innovation which is rapid. In cloud environment, designers of software develop and design applications according to the services being offered by the cloud providers and to what extent we can modify the resources provided to the users. As the essence of cloud is shared resources as seen in the definition are given according to the requirement and the users are billed on pay-per-use [1]. Cloud Computing is to be considered as benchmark to achieve resource on demand. The services models provided by cloud providers are of 3 types [2]. The first model is, Software As A Service (SAAS) gives access to a cloud program which can be used at many places as a complete services, e.g. CRM (Customer Relationship Management) and ERP [3]. Platform As A Services (PAAS) is a service which offers platform for making or managing applications on it, e.g. Google App Engine [4]. Infrastructure as a Service (IAAS) can be defined as a service which gives or helps access virtualized resources over internet. It gives us a workplace for releasing, running, and handling VM's and Storage. It gives modern scalability of calculating resources and on demand storage. Service providers like IBM, Microsoft (AZURE), Amazon, etc. manage these services. According to Gartner [5], cloud computing is defined as ''a style of computing, where massively scalable IT- enabled capabilities are delivered as a service to external customers using Internet technologies.", As per the guidelines for cloud computing and definition given by Seccombe [6] and National Institute of Standards & Technology [7], cloud has four deployment models which can be categorized as Community, Public, Hybrid and private cloud deployment models and also three different delivery models as discussed above, they are the SAAS, PAAS and IAAS. These deployment and delivery (service) models are form the core base of cloud and exhibit many key characteristics like elasticity, scalability, usability, on demand self-service, broad network access, resource pooling, measured services. This paper focuses and discusses the issues related to Cloud environment which a customer or an organization as a whole faces when migrating or adopting cloud technologies. As we know that Cloud is a rapidly evolving technology, it has some legal, security, adoption and negotiable issues to be resolved. Cloud as we know users are billed on usage basis and can be access anywhere over internet. It works as Service on Demand model.

II. Background Work: As we now that cloud computing is the most trending and most used technology now a days, though the research has started late on cloud computing but has been a rampant increase in the papers submitted in the

cloud domain especially in implementation i.e. design and cloud security. On Dec 08', CSA (Cloud Security Alliance) with a goal to provide better security for the cloud computing environment [8]. CSA launched several products to provide security to users. The Multiagency Cloud Computing Forum and The Cloud Computing Interoperability Group have done a lot of progress on delivering control and minimizing security risks by analysing the risk which can be exploited [9]. There are many research and efforts put into cloud environment to increase the effectiveness and usefulness of cloud. It can be noted that the privacy, trust and design are the major issues or challenges we face in the cloud computing domain [10]. In the paper [12] author address security issues in detail and also Security and privacy concerns are discussed in detail in [11].

In [13] it states that cloud computing cannot prosper unless security, privacy, and design issues are resolved. [14] Provides framework for helping cloud users to choose service models according to the requirement and the delivery model accordingly.

III. Adoption Challenges

Adopting or migrating to cloud is the first challenge we face when talking about cloud, when we start developing or moving the existing solution to the cloud then we need to consider or evaluate the pros and cons of this decision and how well it is going to serve our requirements

When should we go for Cloud?

Cloud computing by and large, is a quickly developing strategy for conveying innovation. So, associations considering a move to the Cloud will need to consider which applications they need to move to cloud. In that capacity there are specific arrangements we consider prime plausibility for a hidden move to cloud, these are as follows,

- Figuring Computation needed and here and there likewise other registering related frameworks like PC equipment or calculations, when not tweaked from their unique structure, implying that they are utilized with no customizations or upgrades connected to them, where the arrangement is to a great extent undifferentiated.
- Applications where there is critical exchange between the company or individuals and the outside world. For example, we can take email client etc.
- Applications where there is a significant or absolute need of mobile or web access. Example would be email, ERP or management software.
- Software that is just to be utilized for a fleeting need. An illustration would be joint effort software for a particular undertaking.

- Software where we need to scale the product according to the users flow, i.e. where demand fluctuates. Example would be Taxing software, Bill payment software etc.

Basically organizations must decide whether they need to move or develop an application according to the requirements and constraints involved in the project for example if a project resources utilization changes according to time we need scalability and elasticity and also we need elasticity hence can choose Cloud Environment.

Where Cloud May Not be the Best Option

As we discussed above cloud may be the best option out there but in some situations it is not the best option to choose from because of some concerns which arise as per requirements of the project.

- In some Application we need extremely fast processing is required on the real time data present, it cannot be achieved by cloud to the expected efficiency.
- In some parts it is illegal to host data externally
- In some situations the solution present will be satisfying the need of the organization as per the requirement without any problems hence need not invest into new technology and get nothing, can scale as per the requirement later.

Hence this is a challenge which needs to be addressed before proceeding any further, because if moving to cloud does not meet or does not add any value to the previous or new solution there is no point in migrating or adopting cloud.

IV. Security Challenges

Security, Privacy and trust are the main challenges or issues one need to address before going to develop or adopt to the cloud environment as it encompasses a variety of technologies including resource sharing and allocation, cloud networks, os, virtualization, transaction management, encryption, concurrency control, serialization, load balancing and memory management, etc. Let's us discuss in detail how different issues regarding to security of cloud affects customers and also solutions to them.

A. Authenticity/Identity Management

Identity management or authenticity of customer is utmost importance in cloud since there are using the shared pool of resources and everything can be accessed by other users if not managed properly, it refers to accountability of provider where he cannot modify the information directly and indirectly and also needs to check for the identity of customer before giving access to them. Integrity is a major issue faced by the cloud environment. Essence of cloud is the data stored at different geographies and then transferred to other places an authentic system must be in place to ensure

integrity of data which can stop unauthorized users to stop using data. This problem can solved by using many traditional techniques such as digital signatures and also other methods proposed are access control scheme discussed in [15] uses a decentralized and also a robust access control mechanism where authentication is done without knowing the user's identity. By suing cryptographic Techniques Information is decrypted by only the authentic users. Other Systems include 2 step verification where a specific codes are sent to individual user phone to check the access rights of customers.

B.Key Management

We discussed Encryption above and the methods discussed above all use keys to encrypt and also decrypt the info. Managing those keys also a major issue in cloud since those are the main base of access to information. Storing keys on same cloud is not correct and storing multiple keys becomes a large task. Otherwise storing it on separate database removes the main reason to choose cloud hence we can eliminate that option. The solution which is best to this problem is by using two level encryption which is discussed in [21] for key management.

C.Trust

Trust is the first and foremost parameter to be addressed between customer and service provider's efficient and effective use of cloud computing. Customer always has a doubt whether the service is trustworthy and also whether the private data which is being uploaded to cloud is secure from any exploits, attackers or not. There are SLA's (Service Legal Agreement) which can solve this issue which is being followed from long time. SLA is an agreement between customer and provider which describes the offerings of provider and the future plans [20]. Although this can solve the trust tissue but there are no standards for SLA's.

There has been many solutions proposed to resolve trust issues in recent times some of them are as follows, Trust rating mechanism is proposed in [16] to secure cloud computing environment with the collaboration or help of social media. A Trust model is proposed in [10] to improve security and trust of customer and interoperability of cloud. A framework for SLA [17] is taken to propose a trust management model in cloud environment.

D. Confidentiality

Confidentiality can be defined as a parameter to describe the confidence in provider for preventing any information or data disclosure. Many Methods are prevalent to preserve the user confidentiality and also protect identity of the customers who doesn't want to be exposed, for example encryption is most widely used. Main problem with cloud is

that data is stored in many dispersed locations which can be accessed by many individuals because of the unified architecture of cloud environment.

A new approach is proposed by Hwang, Kai, Sameer Kulkareni, and Yue Hu. [19] it proposes using hierarchy of P2P system of reputation to ensure privacy. It obtains it because of virtualized environment. To ensure privacy a secure cloud computing storage service is proposed and built with the help of cryptographic technique's hence here privacy is being ensured and other cryptographic techniques are also developed to preserve privacy hence giving confidentiality to customers.

E. Encryption

Encryption as we all know is the most important way of securing important and private data so that it can only be accessed by users for whom it is intended. It is also most used technique in cloud computing. Although there have been many drawbacks such as high computation time or other known problems with encryption it is the most used technique and many methods have been developed to decrease the computation time required for encryption or decryption hence increasing throughput.

In [15] a new technique for encryption is proposed to improve efficiency and hence protect data, "End-to-end policy based encryption" is the technique which uses different policies and encrypt and decrypt data according to the policies. Decryption keys are given by Trust Authority and hence enabling the user's to get private access to the clouds. Other methods are also proposed such as Homomorphic encryption which can be applied in cloud computing environment security.

F. Multi tenancy

The essence of Cloud Computing as explained above in introduction is Multi Tenancy where different resources and services are shared all the user of the cloud environment in applications, users at different geographic locations. This will be done to solve the issues of resource distribution to solve scarcity of resources and to decrease the cost to customer allowing him to scale as per requirement.

Hence by sharing confidentiality of the information of different organization will be a risk. Hence isolation must be done to ensure confidentiality, else will be a big loophole in the providers offering Cloud computing environment must have traditional security improvement techniques combined with new technologies such as Intrusion detection system to keep data safe.

G. Data splitting

As we have seen that key management and encryption on its own is a tedious operation and alternative to it is Data Splitting it is fast and also reliable than encryption. Data splitting as the name suggests split the data over multiple hosts that are non-connected.

When the user need to access data, he has to access all service providers to recollect his original data. But there are security issues also involved.

In [20] a model is proposed for efficient and reliable use of data splitting, Multi-Cloud Database Model is the method for data splitting where many clouds and many other techniques are used to ensure the integrity, authenticity of data after the split of data. Hence by using these technique data is stored and replicated according to some parameters and hence decreases intruder's attacks on the cloud.

H. User level issues

Provider must make sure that because of accidental doings of users data must not be lost there must be solution to address accidental deletion and recovery of data to ensure integrity and layered memory management and other issues that may arise due to user access to data should be avoided such as data theft, illegal data access as discussed above etc.

I. Infected applications

Service supplier ought to have the full access to the server with all rights with the end goal of observing and support of server. So this will keep any vindictive client from transferring any contaminated application onto the cloud which will extremely influence the client and distributed computing administration.

J. Backup of data

Traditional Backup Methods which are being used are for legacy systems where earlier desktop or specific applications are used and data centres were designed for consumer's application usage and they cannot be totally applicable to the cloud environment, they are to a point applicable but cannot be used to absolutely confident about data recovery.

Vendor needs to constantly update the sensitive and required information to the backup service so that the data can be backed up in case of any problems, and the data backup must be encrypted so that data will not be accessible outside the environment or other attackers.

V. Legal Issues

Now we move to the Legal Issues which can arise in cloud computing environment, which are most common and also contribute significantly to the decision process of migrating or adopting cloud technologies. These arise between customer and service provider due to contracts which are to acceptable to both parties.

K. Protection of information

When discussing Protection of information of the customer there are some parameters which needs to be addressed mainly Security, Privacy, Data loss etc.

Security: There are some laid out documentation which providers must follow and can be found at Defence Signals Directorate's "Cloud Computing Security Considerations" for a laid out approach to be followed on the issues which may arise in the security domain.

Privacy: for privacy issues providers must provide a transparent plan and the methods which will be undertaken to protect customer privacy and also must declare further actions which will be taken and compensation that will be given in case of discrepancies.

Data loss: Data loss happens due to the error on vendor side and due to some mistakes in their policies which may cost customers a huge loss and also further more loss of trust from their customers hence should be a laid out compensation form to deal with these situations.

L. Liability

In traditional information technology agreements, cloud service agreements typically seek to minimize the provider's liability for any loss that arises from the provision of the service.

By and large, four surely understood components of an obligation claim should be satisfied with a specific end goal to effectively start a legal activity:

- Causality between the demonstration carried out and the harm brought about
- Event of a quantifiable damage
- Issue for the benefit of the cloud computing supplier in type of purpose or gross/light carelessness
- In a case in view of non-satisfaction of a particular commitment under an agreement the absence of execution will be sufficient to set up a reason for activity for rupture of agreement.
- Unlawful act of cloud computing service provider

And before acting or commencing to take legal action on service provider, applicable laws must be determined and see if contract voids them [23]

M. Performance management

Service level agreement (SLA) between customer and provider must specify the performance management clause where customer ensures that the service provider acts or meets according to the agreement at all times, to the level organization needs the performance.

This is important when the performance is utmost importance to the organization and it decides the clients requirements is met or not [24].

VI. Other Issues to be Addressed

Apart from above issues and challenges there are other parameters or issues which are to be sorted out before engaging with a vendor, for migrating or adopting to cloud of a service provider. These are specifically negotiables which are to discussed and agreed between customer and service provider before engaging into business with each other they are, in [25] negotiable parameters are discussed that are

- Service Level Agreements (SLA).
- Exit strategy.
- What will happen to the data of the user if contracts are terminated
- Strategy to change service model both by customer and Service provider.
- Liability for damages to data and service interruptions
- Availability of cloud along with data at all times
- Intellectual property rights
- Service Termination

These issues and questions must be answered by both service providers and customer must negotiate what they want and hence clearing the air between them without any expectations that may or may not be provided which will cause problems to both sides.

VII. Conclusion

As the fundamental reason for Cloud computing is to give resources on demand. cloud computing is a general term which gives an assortment of services from Foundation as IAAS at the base, PAAS as development tool, SAAS as service on demand. It's more essential to comprehend the idea of cloud computing for the companies, and select a

suitable Provider according to their necessity and requirements, and in this study we have discussed the security, adoption, liability and negotiation issues and challenges faced in cloud computing and also the possible solutions are also discussed. As the cloud computing is in evolving stage and hence the security and trust implications are hence these implications are to be resolved eventually. The strong and mutual relation between service provider and customer is solution many of the problems, which can be solved by dialogue by getting mutual benefit. Solution to all cloud computing issues and challenges these issues can be development of a framework which is used to monitor the cloud computing management software.

Acknowledgement

We would like to thank Prof. Manjula R, Ph.D., Associate Professor School of Computer Science and engineering (SCOPE), VIT University, Vellore, for the guidance and support, we received for this work.

References

1. Armbrust, A. Fox, R. Gri_th, A. D. Joseph,R. Katz, A. Konwinski, G. Lee, D.Patterson,A. Rabkin, I. Stoica, and M. Zaharia. A view of cloud computing. Commun. ACM, 53(4), 50-58, Apr. 2010.
2. Y. Amanatullah, C. Lim, H.p. Ipung, A. Juliandri, ―"Toward Cloud Computing Reference Architecture: Cloud Service Management Perspective", ICT for Smart Society (ICISS), 2013 International Conference, 2013, pp. 1–4.
3. M. Cusumano. "Cloud Computing and SaaS as New Computing Platforms", Communications of the ACM, 53 (4), 2010, pp. 27–29.
4. E. Ciurana. ―Developing with Google App Engine‖, Apress, Berkeley, CA, USA.
5. Heiser J. (2009) "what you need to know about cloud computing security and compliance", Gartner, Research, Id_number: G00168345.
6. Seccombe A.., Hutton A, Meisel A, Windel A, Mohammed A, Licciardi A, (2009). Security guidance for critical areas of focus in cloud computing, v2.1. Cloud Security Alliance, 25 p
7. Mell P, Grance T (2011) The NIST definition of Cloud Computing. NIST, Special Publication 800–145, Gaithersburg, MD
8. Messmer, Ellen (March 31, 2009). "Cloud Security Alliance formed to promote best practices". Computerworld.Retrieved May 02, 2014.
9. Onwubiko, Cyril. "Security issues to cloud computing." Cloud Computing. Springer London, 2010. 271-288.

10. Li, Wenjuan, and Lingdi Ping. "Trust model to enhance security and interoperability of cloud environment." In Cloud Computing, pp. 69-79. Springer Berlin Heidelberg, 2009.
11. Ko, Ryan KL, et al. "TrustCloud: A framework for accountability and trust in cloud computing." Services (SERVICES), 2011 IEEE World Congress on. IEEE, 2011.
12. Pearson, Siani, and Azzedine Benameur. "Privacy, security and trust issues arising from cloud computing." Cloud Computing Technology and Science (CloudCom), 2010 IEEE Second International Conference on.IEEE, 2010.
13. H. Takabi, J.B.D. Joshi, G. AhnSecurity and privacy challenges in cloud computing environments. IEEE Security & Privacy;, 8 (6) (2010), pp. 24–31
14. Onwubiko, Cyril. "Security issues to cloud computing." Cloud Computing. Springer London, 2010. 271-288.
15. Yu, Shucheng, et al. "Achieving secure, scalable, and fine-grained data access control in cloud computing." INFOCOM, 2010 Proceedings IEEE. Ieee, 2010. Pearson, Siani, et al. "End-to-end policy-based encryption and management of data in the cloud." Cloud Computing Technology and Science (CloudCom), 2011 IEEE Third International Conference on. IEEE, 2011.
16. Wooten, Ryan, et al. "Design and implementation of a secure healthcare social cloud system." Cluster, Cloud and Grid Computing (CCGrid), 2012 12th IEEE/ACM International Symposium on.IEEE, 2012.
17. M. Alhamad, "Conceptual SLA Framework for Cloud Computing", Accepted for IEEE DEST 2010 on 15 March 2010 2010.
18. Narayan, Shivaramakrishnan, Martin Gagné, and Reihaneh Safavi-Naini. "Privacy preserving HER system using attribute-based infrastructure." Proceedings of the 2010 ACM workshop on Cloud computing security workshop. ACM, 2010.
19. Hwang, Kai, Sameer Kulkareni, and Yue Hu. "Cloud security with virtualized defense and reputation-based trust mangement." Dependable, Autonomic and Secure Computing, 2009.DASC'09.Eighth IEEE International Conference on.IEEE, 2009.
20. AlZain, M., Soh, B., & Pardede, E. (2012). A New Approach Using Redundancy Technique to Improve Security in Cloud Computing. IEEE.
21. Wang, Guojun, Qin Liu, and Jie Wu. "Achieving fine- grained access control for secure data sharing on cloud servers." Concurrency and Computation: Practice and Experience 23.12 (2011): 1443-1464.

22. Zaigham Mahmood, "Data Location and Security Issues in Cloud Computing", International Conference on Emerging Intelligent Data and Web Technologies, 2011.
23. Weber R.H. & Staiger D.N., "Cloud Computing: A cluster of complex liability issues", (2014) 20(1) Web JCLI.
24. Negotiating the cloud – legal issues in cloud computing agreements Commonwealth of Australia 2012, ISBN 978-1-922096-05-0
25. W. Kuan Hon, Christopher Millard and Ian Walden, "Negotiating cloud contracts", Stanford Technology Law Review, Jan. 2011.