IJCSE International Journal of Computer Sciences and Engineering Open Access

Review Paper Volume-4, Issue-4 E-ISSN: 2347-2693

Barriers Faced In Cloud Computing Adoption

Isra Masood[1*], Ankur Bhardwaj[2] and Pushpneel Verma[3]

[1,2,3] Department Of Computer Science and Engineering, Bhagwant Institute of Technology, Dr. APJAK Technical University, Lucknow

www.ijcseonline.org

Received: Mar/29/2016 Revised: Apr/07/2016 Accepted: Apr/22/2016 Published: Apr/30/ 2016

***Abstract*--Cloud computing is the next generation of internet-based comprehensive computing systems which in it, the computing resources are provided "as a service". Cloud computing is an important structure with great potential in lessening the costs by recuperating and developing functionality and cost-effective outcome which in turn can increase cooperation, rate and scalability acceptance to comprehensible degree. This technology has provide large organizations and IT companies with lots of opportunities in developed countries but these opportunities face many challenges and barriers which is one of the main concerns in cloud computing field. This paper focuses on a range of considered issues from a broad cross section of areas of expertise required to ensure a successful cloud computing adoption. It presents in detail the various factors which are key to a successful cloud computing adoption. It also explains how the prominence on collaboration between clients and vendor is necessary for successful adoption of cloud computing. If the organisation feels free, confident and secure to use cloud services then it is more likely that the adoption rate will increase. As Cloud Computing is referred to both the applications delivered as services over the Internet and the infrastructures (i.e., the hardware and systems software in the data centres) that provide those services , we present the security concerns in terms of the diverse applications and infrastructures. More concerns on security issues, such as availability, confidentiality, integrity control, authorization and so on, should be taken into explanation. The rest of the paper will be organized as highlighting the basic cloud computing definitions and architecture, presenting the barriers and challenges to adoption of cloud computing and then the paper will be concluded along with the future research scope.**

Keywords: cloud; organisational challenges; adoption; SLA's

I. INTRODUCTION

With exceptional adoption in industry over the past few years, cloud computing continues to be one of the most vital and fast-growing models in IT. Cloud computing is "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction.[1]" Cloud computing is based upon a service-based architecture wherein services are provided mainly at the infrastructure level (e.g., virtual machines, storage) platform level (e.g., database, web server), or software level (e.g., email, ERP solution). Despite the widespread adoption of cloud computing, researchers and practitioners have been actively reporting issues and challenges with this new technology. Some of the challenges seem to be fundamental such as issues with privacy and security. Other challenges such as sub- optimal performance and limited bandwidth are a natural result of pushing the boundaries of this new model to achieve more. The goal of our research is to gain an understanding of the type of issues and challenges that have been emerging over the past years.

II. CLOUD COMPUTING DEFINITION AND FEATURES

A number of computing researchers and practitioners have attempted to define Clouds in various ways. Here are some definitions: NIST definition of cloud computing: " Cloud computing is a model for enabling 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". Buyya defined Cloud as follows: "A Cloud is a type of parallel and distributed system consisting of a collection of inter-connected and virtualized computers that are dynamically provisioned and presented as one or more unified computing resource(s) based on service-level agreements established through negotiation between the service provider and consumers." To understand the importance of cloud computing and its adoption, one must have to understand its principal characteristics, its delivery and deployment models.

A. Characteristics

The five key characteristics of cloud computing defined by NIST [2] includes:

- On-demand self-service: A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed without requiring human interaction with each service's provider.
- Ubiquitous network access: Accessed through standard mechanisms on heterogeneous thin and thick clients. Both high bandwidth and low latency are expected.
- Location-independent resource pooling: The provider's computing resources are pooled to serve all consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.
- Rapid elasticity: Lets us quickly scale up (or down) resources.
- Measured service: are primarily derived from business model properties and indicate that cloud service

providers control and optimize the use of computing resources through automated resource allocation, load balancing, and metering tools.

B. Cloud Computing Service Model

Three cloud computing delivery service models are:

- *Software as a Service (SaaS):* In SaaS, the business application software are delivered to customer/client as on-demand services. Because clients acquire and use software components from different providers, so the main issue is here that information handled by these composed services is to be well protected. Example of SaaS providers are Salesforce, GoogleApp etc.
- *Platform as a Service (PaaS)*: PaaS provide an application or development platform in which user can create their own application that will run on the cloud. Microsoft Azure, Manjrasoft Aneka and Google AppEngine are examples of PaaS providers.
- *Infrastructure as a Service (IaaS)*: Iaas is the delivery of computer hardware like servers, networking technology, storage, and data centre space etc. as a service. It may also include the delivery of operating systems and virtualization technology to manage the resources. Example is Amazon S3, EC2, and OpenNebula etc.

C. Cloud Deployment Models

There are four cloud deployment models:

- *Public cloud*: In public cloud, the resources are dynamically provisioned on a fine grained, self-service basis over the Internet, via web applications/web services. The customers can quickly access these resources, and only pay for the operating resources. As multiple customers are sharing the resources so major dangers to public cloud are of security, regulatory compliance and Quality of Service (QoS)
- *Private cloud*: In the private cloud, computing resources are used and controlled by a private enterprise. In private cloud, resource access is limited to the customers that belong to the organization that owns the cloud. The main advantage of this model is that the security and privacy of data is increased as compliance and QoS are under the control of the enterprises.
- *Hybrid cloud:* A third type can be hybrid cloud that is typical combination of public and private cloud. Through this environment an organization can provide and manage certain resources in-house and have others provided through external resources.
- *Community cloud*: The cloud infrastructure is shared among a number of organizations with similar interests and requirements. This may help limit the capital expenditure costs for its establishment as the costs are shared among the organizations. The cloud infrastructure could be hosted by a third-party vendor or within one of the organizations in the community. Although, cloud computing is becoming a well-known buzzword nowadays. However, security issues present a strong barrier for users to adapt into Cloud Computing systems. According to an IDC survey in August 2008, security is regarded as the top challenge of Nine.

III. CLOUD ADOPTION CHALLENGES

A. Security challenges

The reality of security is based on the probability of different risks and how effective the various mitigation strategies are in place in dealing with the perceived risks. Cloud computing and cloud service providers need to address a number of challenges that affects security in the cloud [4]. How these challenges are addressed and how the mitigation plans are put in place is crucial in ensuring that clients trust cloud computing environment. The challenges that need to be addressed are as follows:

- Loss of governance: By using cloud services the client passes control to the provider. This passing off, of control to the provider, results in loss of control over a number of issues which in turn may affect the security posture of the client data and applications. This is aggravated by the fact that SLAs may not tender commitment on the part of the provider, and thus widening the security cover gap.
- Lock-in: Lack of tools, procedures and standards for data format or service interfaces that could guarantee portability and interoperability between applications and services and between vendors is another hurdle.
- Isolation failure: failure for separate storage mechanisms and reputation between diverse tenants also raises question on attacks such as guest hopping attacks and how they can be dealt with.
- Malicious insiders**:** sometimes the architecture of cloud computing environment creates certain roles which aggravate the risk of insider attack.
- Insecure or incomplete data deletion: What happens when a client requests to delete a cloud resource? Is there possibility of partial deletion? How timely is the deletion made? Given the nature of cloud computing these questions have no straight answers.
- Data interception: Given the distributed nature if cloud computing architecture, the amount of data in transit is increased greatly as opposed to conventional computing environment. This makes cloud computing more susceptible to attacks such as: replay attacks, man-in-the-middle attacks, sniffing and spoofing [13].

B. Legal challenges

With data and application hosted by a third party, the cloud service provider; issues of ascertaining the legal and compliance impact to participating parts is difficult. Issues related to data protection, privacy, jurisdiction of storage and processing and e-discovery raise. It also raises the issue related to the responsibility of the aforementioned issues.

A number of challenges emerge relating to cloud computing. These challenges may be categorised under various names and titles.

- The cloud service customer/provider role: The EU directive puts on the shoulders of data controllers most

of the obligations for ensuring privacy and data protection of the individual, with few on the data processors (EU, 2006, Hustinx, 2010). In the case of cloud computing it is hard to pin cloud providers as data controllers though they process data entrusted to them by the data controller according to the directive. Therefore it is imperative that the role played by cloud vendors and customer be clearly defined to ensure compliance to the directive. The applicability of EU laws: this relates to how cloud vendors will be made to comply with EU laws [5]. Will they need to have their cloud in the EU? Is it mandatory the cloud be located in EU or a country that is compliant? How is this going to be verified?

- Trans-border data flow: The directive demands that data not be transferred outside the EU. Transfer can only take place to countries with adequacy level of protection. It also demands for contracts and notifications in case of transfers taking place. The problem in this case lies in the directive definition of data transfer. The definition is based on a point to point concept of data transfer. With this concept it is difficult in cloud environment to constantly notify and sign contracts as data tend to be constantly moving and changing jurisdictions.
- Ensuring the protection of data: The challenge here is to ensure that both data controller and data processor have effective means of protection for data.

C. Compliance challenges

Nature of cloud computing environment puts at risks industry and/or regulatory requirements. This is because of the difficult to force providers to comply with these regulations or industry standards. For example in using public clouds infrastructure it entails failure to comply with certain requirements such as PCI DSS, Federal Information Security Management Act (FISMA) of 2003, Gram-Leach Billey Financial Services Modernisation Act of 1990 and the European Data Protection Act of 1990 among others. This is made difficult because these acts and regulations were not prepared with cloud computing in mind [9]. They focused of physical asset protection (Hamilton). Compliance is also made difficult as vendors are not necessarily industry specific. This means that vendors may not be required to comply with any industry specific legislation or standard. Another aspect is that vendors may be offering their services to customers from different industry with different compliance requirements.

D. Organisational challenges

Large organisations are more concerned with the value that cloud computing may offer to them rather than just the migration of applications or using cloud computing just as a platform for service delivery[3]. This section will identify and discuss issues surrounding organisation adoption and migration of applications/systems to the cloud in order to satisfy and meet organisations requirements.

- Organisational change: The IT department of most organisations are not used to utility model of service sharing. This type of utility billing for shared resources in an organisation calls for changes in organisation culture and organisation process maturity. An organisation planning for cloud computing adoption should make effort to access and analyse all the possible organisational impact to culture, processes, work relationships and internal politics that cloud computing may bring [8].
- Governance and risk management: The governance and risk management requires organisations to ensure that there are proper mechanisms and processes across the information supply chain that covers cloud providers, customers and other stakeholders, and supporting third parties to vendors
- Systems and application migration: For cloud computing, migrating systems and applications poses a challenge to organisations. The challenges include IT policy formulation, organisational politics and culture. It also includes identifying the system dependencies and how the migration to cloud will affect these dependencies and the work processes in place.
- Service level Agreements (SLA) management: The need for specific SLAs is another challenge. This is a challenge due to the fact that vendors may not always meet the requirements for SLA [12] of an organisation. The potential for down-time and lack or inadequate SLA agreement from some cloud vendors pose a great challenge (Google, 2010, Golden, 2009, Amazon, 2010)
- The Economics of Cloud computing: The costs associated with cloud adoption include (but not limited to) building new technology and security infrastructure that are cloud compatible and redesigning existing ones, training and retraining, institutional realignment, policy and standards formulations in addition to the cost of cloud services which in most cases are not known until the services have been consumed. Other challenges include the capital and operation costs ownership within an organisation [14]. This is because in most organisations the costs related to capital and operations of IT infrastructure are de-centralised and thus are owned by different departments.

IV. CONCLUSION

As the adoption of cloud computing is becoming increasingly common, issues and challenges are still emerging at the various levels of the cloud architecture. This paper discussed the different challenges facing organisations when planning for cloud computing adoption. The challenges discussed are: security challenges, legal challenges, compliance challenges, organisational challenges etc.Other organisation impact includes organisation work procedures and process that have developed over time. Another organisational challenge that have been discussed is the governance and risk management in cloud computing. This includes how organisation can mitigate risks and maintain IT governance in cloud computing that will ensure compliance to both

legal and security requirement. In system and application migration challenge, issues such as organisation politics and ownership, system and application dependencies which may affect how applications are to be migrated to the cloud. In service level agreement management the issue of lack of proper SLA or inadequate SLA impacts on how organisations will use cloud computing while ensuring quality service to customers and without breaching any legal and security compliance. In the economics of cloud computing issues related to pricing and payment models, and internal management of costs are critical.

Thus future work should incorporate a thorough study of all the challenges faced during cloud adoption and devise a strategy or framework which may handle them and allow an efficient adoption of cloud computation by the organisations.

REFERENCES

[1] GRANCE, T. (2010) The NIST Cloud Definition Framework. NIST

[2] Gens, M. Adam, D. Brandshaw, and C. A. Christiansen, "Worldwide and Regional Public IT Cloud Services 2013-2017 Forecast," International Data Corporation, Market Analysis 38, Aug. 2013.

[3] C. Wyld, "THE cloudy future of government IT: Cloud computing and the public sector around the world," Int. J. Web Semantic Technol., vol. 1, no. 1, pp. 1–20, 2010.

[4] P. Black, T. Byron, F. Caio, and A. Chitty, "Digital Britain," The Secretary of State for Culture, Media and Sport and the Minister for Communications, Technology and Broadcasting, United Kingdom, London, United Kingdom, Parliamentary Report, Jun. 2009.

[5] BUYYA, R., YEO, C. S., et al. (2008) Market-oriented Cloud Computing: Vision, Hype, and Reality for Delivering IT Services as Computing Utilities. *10th IEEE*

[6] Finish Cloud Software Program, "Cloud Software (Finland) Guide," 2013.

[7] Mewada, Shivlal, Umesh Kumar Singh, and Pradeep Sharma. "Security Based Model for Cloud Computing." Int. Journal of Computer Networks and Wireless Communications (IJCNWC) 1.1 (2011): 13-19.

[8] Rempel, J. K., Holmes, J. G., et al. (1985) Trust in close relationships. *Journal of Personality and Social Psychology,* 49**,** 95-112.

[9] Mather, T., Kumaraswamy, S., et al. (2009) *Cloud Security and Privacy: An Enterprise Perspective on Risk and Compliance,* Sebastopol, CA, O'Reilly Media, Inc

[10] Jeffrey, K. & Neidecker-Lutz, B. (2009): The Future Of Cloud Computing: Opportunities For European Cloud Computing Beyond 2010; 66

[11] Mewada, Shivlal, Umesh Kumar Singh, and Pradeep Sharma. "Security Enhancement in Cloud Computing (CC)." International Journal of Scientific Research in Computer Science and Engineering 1.01 (2013): 31-37.

[12] CSA (2009) Security Guidance for Critical Areas of Focus in Cloud Computing V2.1.Cloud Security Alliance

[13] CSA (2010): Top Threats to Cloud Computing V1.0; Cloud Security Alliance

[14] B. Mahesh Kumar and V. Savitha, "A Survey on Emergence of Cloud Computing using Brokering Services", International Journal of Computer Sciences and Engineering,Volume-04,Issue-02,Page No(85-91),Feb-2016,E-ISSN: 2347-2693

AUTHOR'S PROFILE

Ms Isra Masood received her Bachelor of Technology in Computer Science and Engineering from Dr. APJ Abdul Kalam Technical University, Lucknow and she is currently working towards the M.Tech degree in Computer Science and Engineering from the same university. She has published many research papers in good National and International journals and conferences. Her main research areas are Computer Networking, Cloud Computing, Software Engineering and Artificial Intelligence.

Mr. Pushpneel verma recieved his Bachelor of Engineering in Computer Science from Dr. B.R. Ambedkar University, Agra. He has also done his M.Tech from the same university. With a working experience of 14 years, he currently holds the position of the Dean in B.I.T. Muzaffarnagar.

Mr. Ankur Bhardwaj received his Bachelor of Technology in Computer Science and Engineering from B.I.T. Meerut and completed his M.Tech from Bhagwant University, Ajmer. He has a working experience of 9 years and is currently the H.O.D. of the Computer Science Department. His research interests is in Green Computing.