CLOUD COMPUTING: DATA MANAGEMENT AND SECURITY

Swati Pandya
M.Tech., Student, PAHER University

ABSTRACT

Abstract

Cloud Computing has come into authenticity as a new IT infrastructure built on top of a series of techniques such as distributed computing, virtualization, etc. Although the new innovative spectacular platform has many benefits that it can bring forth, it also pioneer the difficulty of protecting the security ofdata and information outsourced by cloud users.

Cloud computing changed the world around us. Nowpeople are moving their data to the cloud since data is getting bigger and needs to be accessible from many devices. Therefore, storing the data on the cloud becomes a means to ensure accessibility. However, there are many issues that counter data stored in the cloud starting from virtual machine which is the mean to share resources in cloud and ending on cloud storage itself issues. In this paper, we present those issues that are preventing people from adopting the cloud and give a survey on solutions that have been done to minimize risks of these issues. For example, the data stored in the cloud needs to be confidential, preserving integrity and available. Moreover, sharing the data stored in the cloud among many users is still an issue since the cloud service provider is untrustworthy to manage authentication and authorization. In this paper, we list issues related to management of stored data and solutions to the security issues.

Key words: Cloud Computing, Data management, Cyber Security

INTRODUCTION

Enterprises are driving towards less expenditure, more accessibility, and quickness, managing risk and threats - all of which is moving towards Cloud Computing. Cloud is not a particular product, but a way of delivering IT services that are consumable on demand, elastic to scale up and down as needed, and follow a pay-for-usage mode. IT (Information Technology) revolution is driving technology to a new arena from time to time. The Internet is one of the most popular technology now-a-days by the elegance of IT. Now it is on the edge of revolution, where resources are globally interconnected. Hence, resources can be easily shared and managed from anywhere and anytime. Cloud computing is the main element of this standard, that provides a large storage area where resources are available from everywhere to everyone as a service rather than as a product.

Cloud computing provides highly scalable computing environment for an assortment of IT services. It provides services to client individual, to big organizations or companies. As a result, IT departments and individuals are saved application developments, deployments, securities, purchasing new hardware and software and maintenance time and cost effectively. Cloud service helps to reduce power consumption, cooling, storage and uses space for cloud users or consumers in cloud environment. Throughout in the history of computer science various attempts have been made to release users from the needs of computer hardware (such as storage) and software, since time-sharing utilities

envisioned in 1960s, network computers in 1990s and commercial grid computing to

cloud computing in more recent years. Cloud computing comes focus only when think about what IT always needs: a way to increase the capabilities of a system on fly without investing any new infrastructure, training a new personnel and licensing of any new software. Today cloud services provide subscription or pay-per-use based service; the services provide over the Internet in real time, in which extends basic IT capabilities into robust area. Cloud computing compromises wide sequence of applications and upkeep to many technologies, but still it bargains numerous classes of threats to cloud users. Initially, the cloud service supplier which have controls over cloud resources, can access any data existing in the cloud organization.

REVIEW OF LITERATURE

Neelima&Padma (2014) in A STUDY ON CLOUD STORAGE highlighted the fact that Cloud Storage is simply the delivery of virtualized storage on demand and it is more advantageous than traditional storage because of its availability, scalability, performance, portability and its functional requirements. Chowdhury(2014) in her research on Security in Cloud Computing identified major security risks and issues those are required to be considered during deployment and development of services in cloud and the how to mitigate those security risks and issues. Ramgovind,Eloff, Smith (2010) in the paper tried to provide an overall security perspective of Cloud computing with the aim to highlight the security concerns that should be properly addressed and managed to realize the full potential of Cloud computing.

ARCHITECTURE OF CLOUD DATA SERVICE

The system architecture for cloud computing data services is shown in the figure 1. At its core, the architecture consists of four different entities: the data owner, who is also a cloud user and has large amount of details to be stored in the cloud; the cloud user, who is authorized by the data owner to access his data; the cloud server, which is managed by cloud service providers to provide data storage and data sharing services and has significant storage space and computation resources; the third party auditor(TPA), which is the trusted entity that assesses the cloud storage security on behalf of the data owner upon request.

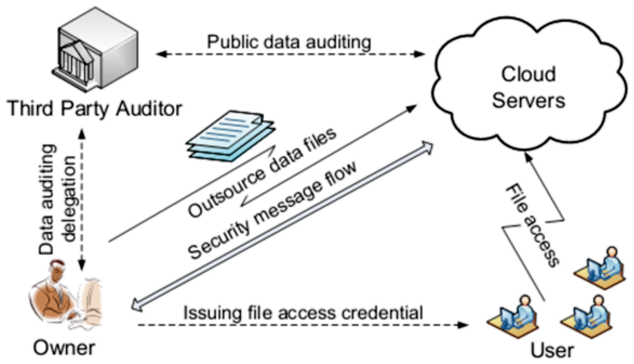

Fig 1:Architecture of Cloud Data Service

Research Objectives

- To study the key benefits of managing data through Cloud Computing
- To highlight the security risks of cloud computing and challenges of data management

Research Methodology

The data was collected from 100 respondents i.e. IT professionals to reveal the benefits, risks and challenges of the new technique of storing data.

BENEFITS OF USING CLOUD COMPUTING

Cloud computing provides huge benefits to the consumers and quantifiable methods to manage the data.

The above graph and table depicts the various benefits of cloud computing and the maximum response was given to the benefit of cost efficiency which is the fact that is responsible for the popularity of its usage. Around 43% professionals agreed that cost minimization and 21 % were of the opinion that agility are the two main benefits derived from the use of cloud technique

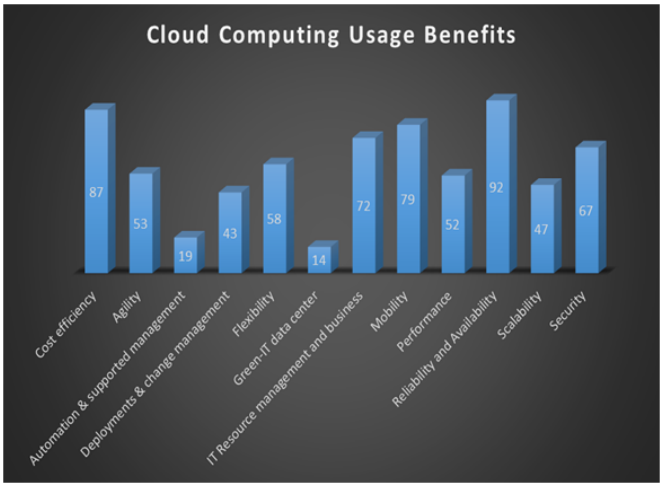

Fig. 2: Benefits of using Cloud Computing

Risk Area	Critical	Somewhat Important	Not so Important	Ranking
Information Security	86.40	13.60	0.00	First
Change Management	61.40	38.60	0.00	Second
Disaster Recovery	36.40	63.60	0.00	Third
Interface Management	36.40	55.30	8.30	Third
Operations Management	36.40	43.39	20.21	Third
Regulations And Legislation	28.00	49.00	23.00	Fourth
Third Party Management	4.00	52.30	43.70	Fifth

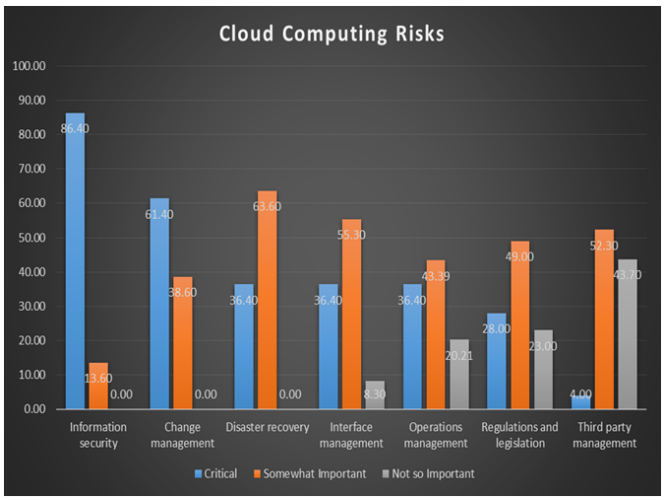

Fig.3: Cloud Computing Risks

The respondent's opinion about the risks in the usage of cloud showed that the foremost risk is information security risk i.e, to ensure security of the data stored in the cloud and second most threating risk is managing the change that is requiread for successful implementation the technique in business activities. Other risks include disaster recovery, interfacemanagement, operations management and lowest ranked risks are regulations and third party management.

Table 2: Challenges of data management in cloud computing

Issues or Challenges of the CLOUD	Percentage
Not enough major suppliers yet	44.3%
Regulatory requirements prohibit cloud	49.2%
Worried on-demand will costs more	50.4%
Not enough ability to customize	55.8%
Hard to integrate with in-house IT	61.1%
Bringing back in-house may be difficult	50%
Lack of interoperability standards	0%
On-demand payment model may cost more	0%
Performance	63.1%
Availability	63.1%
Security	74.6%

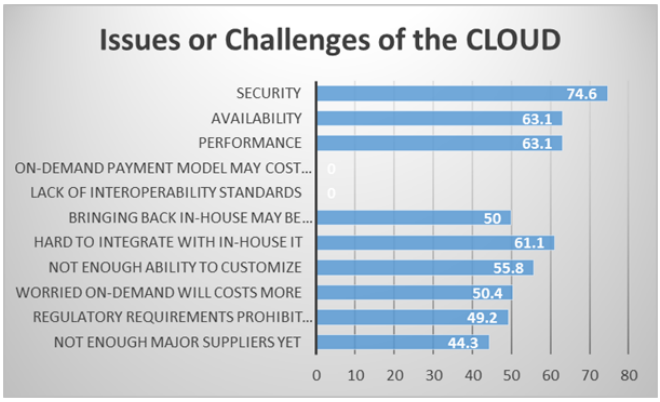

Fig.4: Challenges faced in using Cloud Computing

The challenges of cloud computing are very threatening and the response of almost 75% respondents reveal that security is the most vital challenge to be conquered followed by availability and performance

MANAGING CLOUD COMPUTING SECURITY

In order to effectively manage and control the use of cloud technology in an organization, 2 things are to be covered

1. Decision makers need to assess the potential impact of Cloud computing on their competitive edge.
2. Security questions of implementing cloud technologies will then be needed to evaluate.

Managing and controlling Cloud issues will need to address but not limited to the following:

- How the organization will deal with new and current Cloud compliance risks.
- How Cloud computing may affect the organization in terms of its business intelligence and intellectual property.

A. Cloud Governance

Cloud computing policies and procedures should be put in place in an effort to protect the cloud from potential of threats, hacks and the loss of information.

B. Cloud Transparency

Transparent security would entail cloud providers disclosing adequate information about their security policies, design, and practices, including disclosing relevant security measures in daily operations. One of the most important protocols ensuring transparency within Cloud computing is the SLA which is the only legal agreement between the service provider and client. The main aspects as a guideline, which the SLA contains, are:

- Services to be delivered, performance,
- Tracking and Reporting
- Problem Management
- Legal Compliance
- Resolution of Disputes Customer Duties
- Security responsibility
- Confidential Information Termination.

C. Cloud Computing's Security Impact

Users usually fail to realize that they are in fact using an Internet based service instead of computer services to store their data on cloud. This risk of confusion is likely to increase when cloud based apps lack any recognizable browser branding, and continue to function when the user is not connected to the Internet. So the organizations must decide whether proper security measures are taken or do they share a joint responsibility with service providers when engaging in the cloud environment.

Conclusion

Although Cloud computing can be seen as a new phenomenon which is set to revolutionize the way we use the Internet, there is much to be cautious about. There are many new technologies emerging at a rapid rate, each with technological advancements and with the potential of making human's lives easier. Around

43% professionals agreed that cost minimization and 21 % were of the opinion that agility are the two main benefits derived from the use of cloud technique.

However, one must be very careful to understand the limitations and security risks posed in utilizing these technologies. Cloud computing is no exception. In this paper key security risks and challenges which are currently faced in the Cloud computing industry are highlighted. Almost 75% respondents reveal that security is the most threatening risks faced by the users of cloud technology it is a social obligation of government to promote the use of best practices for providing security assurance within Cloud computing, and provide education on the uses of Cloud computing to help secure all other forms of computing. By following certain norms and regulations, a great deal of insecurities may be easily expelled, saving business owners' valuable time and investment. Cloud computing has the potential to become a frontrunner in promoting a secure, virtual and economically viable IT solution and future work and progress lies in standardizing Cloud computing security protocols.

REFERENCES:

- S. Subashini, V. Kavitha, A survey on security issues in service delivery models of cloudcomputing, Journal ofNetworkand Computer Applications, vol. 34, Issue 1, pp. 1-11, 2011.
- M.Carroll, A.Van der Merwe, P.Kotze, Secure cloud computing: Benefits, risks and controls, Information Security South Africa (ISSA), pp. 1-9, September 2011.
- S. Subashini, V. Kavitha, A survey on security issues in service delivery models of cloud computing, Journal of Network and Computer Applications, vol. 34, Issue 1, pp. 1-11, July 2010.
- D. Zissis, D.Lekkas, Addressing cloud computingsecurity issues, Future Generation Computer Systems, 2011.
- National Institute of Standards and Technology, NIST
- Cloud Computing Program, 2010<http://www.nist.gov/itl/cloud/>Chonka, Y.Xiang, W.Zhou, A.Bonti, Cloud security defence to protect cloud computing against HTTP-DOS and XML-Dos attacks, Journal o Network and Computer Applications, vol. 34, pp. 1097-1107, 2010.
- Grobauer, T. Walloschek, E. Stocker, UnderstandingCloud Computing Vulnerabilities, Security & Privacy, IEEE, vol. 9, Issue 2, pp. 50-57, March 2011.
- B., Thuraisingham, V., Khadilkar, A., Gupta, M., Kantarcioglu, L., Khan, Secure data storage and retrievalintheclod,Collaborative Computing: Networking, Applications and Work-sharing (CollaborateCom), 2010 6th International Conference on, pp. 1-8, May 2011.
- Z., Chen, J., Yoon, IT Auditing to Assure a Secure Cloud Computing, Services (SERVICES-1), 2010 6thWorld Congress on, pp. 253-259, September 2010.
- J., Wayne, T., Grance, Guidelines on Security and Privacy in Public Cloud Computing, U.S. Department of Commerce, January 2011.

http://csrc.nist.gov/publications/drafts/800-144/Draft-SP-800-144_cloud-computing.pdf [Accessed on: 23 October 2011