International Journal of Research in Engineering and Applied Sciences

Vol. 6 Issue 7, July - 2016

ISSN: 2249-3905 | Impact Factor: 6.573 |Thomson Reuters Researcher ID: L-5236-2015

AN INVESTIGATION OF THE ADOPTION OF CLOUD COMPUTING IN ORGANIZATIONS: SECURITY & CHALLENGES

Jaipal Marripally[1], Dr Arvind Kumar Sharma[2]

Department of Computer Science and Engineering

[1,2]OPJS University, Churu (Rajasthan)

ABSTRACT

Many IT professionals would concur that cloud computing is the most progressive information conveyance show since the introduction of the Internet. For corporate administration and chiefs, cloud computing brings many financial and practical benefits and in addition genuine security worries that may debilitate business continuity and corporate notoriety. The definition of cloud computing is as yet hazy in an extensive part, due to the magnitude of the security dangers and the for all intents and purposes unlimited measure of information being distributed. The reason for this exploration is to survey how cloud security dangers and dangers most normally examined today are affecting present and forthcoming cloud clients' choices on reception.

1. INTRODUCTION

Cloud computing has been envisioned as the bleeding edge perspective in calculation. In the cloud computing environment, the two applications and assets are passed on ask for over the Internet as services. Cloud is an area of the equipment and programming assets in the server cultivates that give different services over the framework or the Internet to satisfy customer's necessities. The illumination of "cloud computing" from the National Institute of Standards and Technology (NIST) is that cloud computing empowers inescapable, accommodating, on-ask for network access to a shared pool of configurable figuring assets (e.g., frameworks, servers, stockpiling, applications, and services) that can be immediately provisioned and released with irrelevant administration effort or supplier center association.

2. CLOUD COMPUTING SERVICE ARCHITECTURE

Cloud architecture, the systems architecture of the software systems involved in the delivery of cloud computing, ordinarily involves multiple cloud segments communicating with each other over a free coupling instrument, for example, a messaging line. The services given to the purchaser by the cloud infrastructure depend on the integration of the following three service architectures (additionally alluded to as service models).

- "Infrastructure as a Service (IAAS)" – service supplier bears all the cost of servers, network hardware, storage and back-ups. The clients simply need to pay to take the computing service and construct their own particular application software. Amazon EC2 is an extraordinary case of this sort of service.
- "Platform as a Service (PAAS)" – service supplier just give platform or a pile of answers for the clients. It helps clients saving investment on hardware and software. Google engine and Force.com give this kind of service.
- "Software as a Service (SAAS)" – service supplier will give the clients the service of using their software, particularly any kind of use software. Google (GOOG), Salesforce.com (CRM Customer Relationship Management), Net suite are a portion of the cases.

The abnormal state architecture of cloud computing is delineated in Figure 1.2. The cloud supplier invests in the hardware infrastructure and fabricates the three service architecture layers over it. The IAAS is conveyed straightforwardly upon the hardware and PAAS is coupled above it. The SAAS is filled in as a best layer. As of late, there is one more level of reflection that is given over these three layers. This layer empowers arrangement of Business Process as a Service (BPAAS). The existing and outsider services are vertically combined with these service layers. The cloud supplier empowers legitimate integration between the layers to empower the cloud system to give every one of the services to the consumers either individually or in a coupled manner.

Barriers to Cloud Computing Adoption in the Enterprise

Despite the fact that there are many benefits to adopting cloud computing, there are likewise some huge barriers to its adoption. Be that as it may, it is essential to in any event get out what a portion of the other barriers to adoption are:

- Security
- Privacy
- Connectivity and open access
- Reliability
- Independence from CSPs
- Interoperability
- Economics esteem
- IT governance
- Changes in the IT association
- Political issues because of worldwide limits

Vol. 6 Issue 7, July - 2016

ISSN: 2249-3905 | Impact Factor: 6.573 |Thomson Reuters Researcher ID: L-5236-2015

3. PROBLEM STATEMENT

A few security management principles and measures have been expected to protect the cloud however by the by cloud security is at a high risk because of the innovative hacking procedures. These security principles contain Information Technology Infrastructure Library (ITIL) rules, ISO/IEC 27001/27002 standard and Open Virtualization Format (OVF) models. The dull side of this photo is that; in spite of having such measures we can't guarantee cloud security. This hard reality has two clarifications; one is the shortcomings in these security schedules as of now received everywhere throughout the globe and besides the innovative hacking strategies that are rapidly winding up plainly exceptionally keen, complex and difficult to identify.

4. OBJECTIVES

- To study the cloud computing environment and its infrastructure
- To study the role of cloud computing architecture in the business & public sector
- To study the benefits & challenges of cloud computing in companies
- To study the solutions for improving the security over cloud computing in the organization

5. RESEARCH DESIGN& PROCEDURE

A total of 131 responses were received over a period of five weeks from September to mid-October in 2016. Respondents came from various company sizes and industries, and nearly 35% of the respondents indicated that their organizations are currently using public cloud computing, while many others are prospective cloud users.

Because of the technical terms used in the survey and the requirement for fundamental knowledge on cloud computing, quite a few respondents chose not to complete the survey. Completion ratios for each survey section were as follows:

1) Part 1: Current cloud computing usage – 72.5%
2) Part 2: Security concerns – 56.5%
3) Part 3: Defensive measures (presented to current cloud users only) – 31.3%
4) Part 4: About respondent's organization and comments – 53.4%

Because all survey questions were either single-choice or multiple choice questions except for one open-ended comment field at the end, no responses were rejected as long as an answer choice was made. Because the survey was advertised and mass-solicited online, the response rate is unknown.

Vol. 6 Issue 7, July - 2016

ISSN: 2249-3905 | Impact Factor: 6.573 |Thomson Reuters Researcher ID: L-5236-2015

6. DATA ANALYSIS

After information gathering was finished, responses were separated from Qualtircs as a comma delimited document, and afterward stacked to a Microsoft SQL Server 2008 R2 database for advance analysis. Qualtircs' worked in reports and cross-arrangement functions were also used to create response counts and correlations between security question responses and statistic information. Charts and graphs were created by trading responses to an Excel document. Because of the business-and practical arranged nature of this small survey and absence of numerical information being gathered, no statistical bundle software such as SPSS was used in information analysis. The conversion of the Likert scale values to numeric points was executed.

7. RESULTS & DISCUSSION

Security Risk and Threat Awareness

In the security risk and danger awareness questions, somewhat more than 80% (61 of 74 respondents) demonstrated that their organizations knew about security issues associated with open distributed computing. This is a reasonable level of awareness considering the measure of consideration cloud security is accepting these days, as well as more organizations considering data security important because of pressures from administrative guidelines and protection concerns of the general population. 65% (48 of 74 respondents) demonstrated their organizations were lessConcerned with malicious insiders than outside attackers.

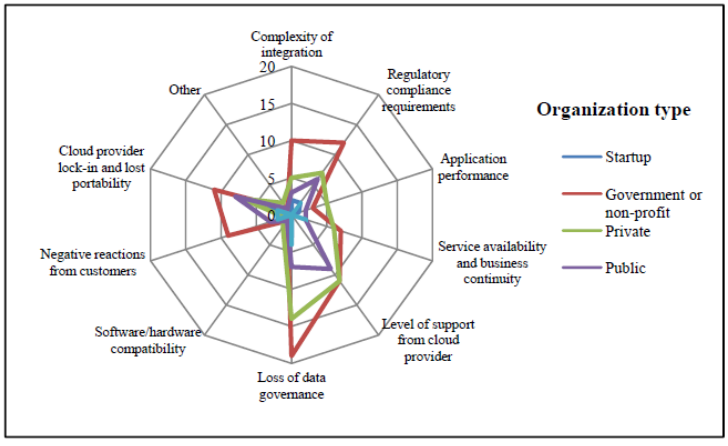

Figure 1 Primary concerns for cloud adoption by organization type

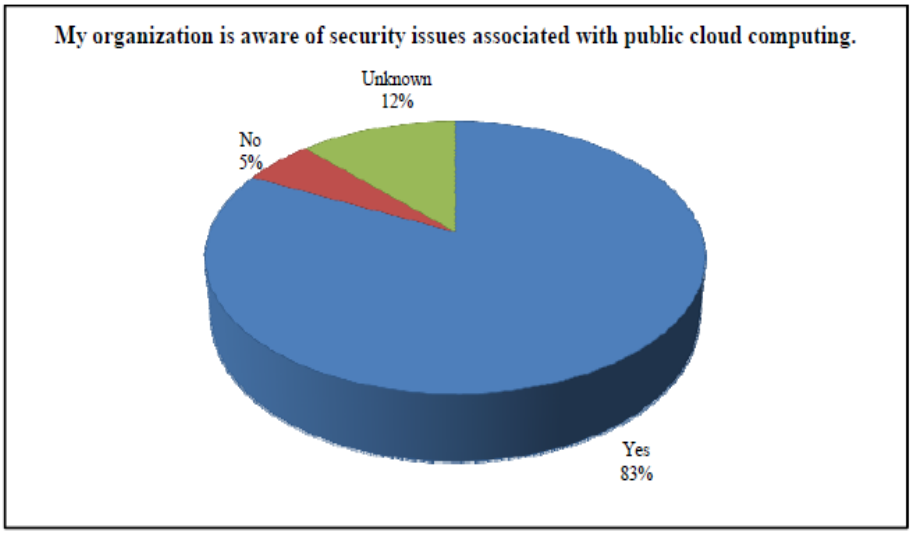

Figure 2 Security issue awareness

This is also sensible because most noticeable cloud security related incidents announced have been because of exploits starting from outside the casualty organizations. Around half (39 of 74 respondents) showed certainty with their cloud providers' security capabilities, and knew that there was a reasonable correspondence channel for escalating incidents to their cloud supplier in case of a security rupture (Figures 3 and 4). These are the areas where the merchant user relationships can be enhanced, principally by ensuring all security related concerns are addressed in SLAs. As stated in the previousPart, SLAs should cover occurrence response procedures, support for outages, and money related restitution for lost business.

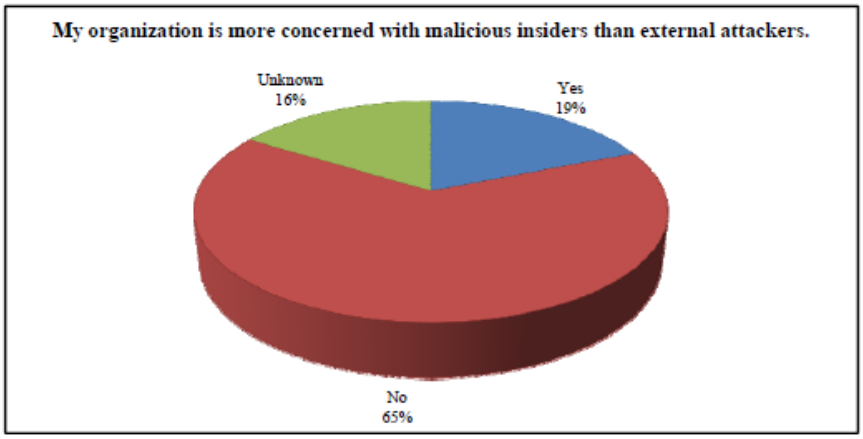

Figure 3 more concerned with malicious insiders

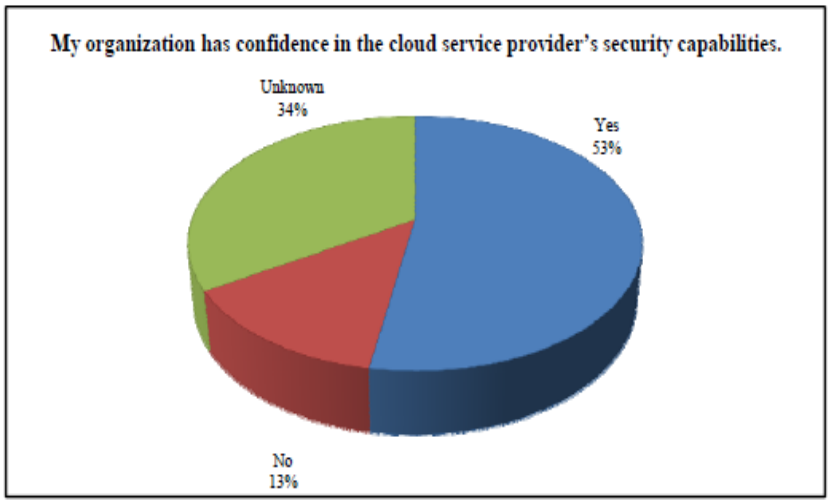

Figure 4 Provider security confidences

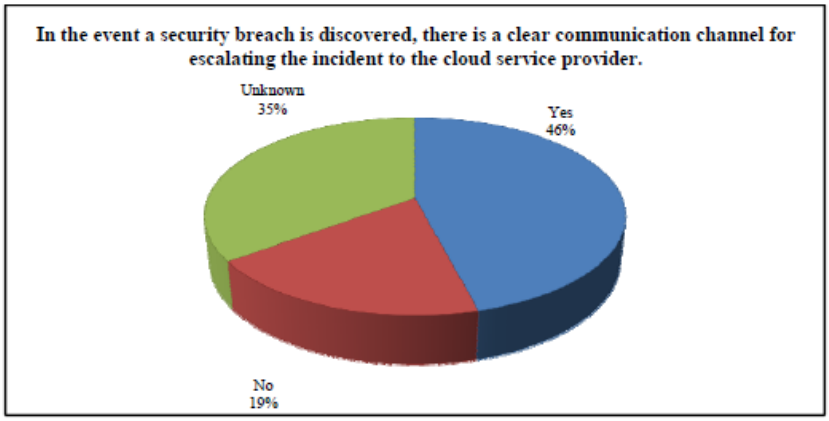

Figure 5 Existence of escalation channel

When contrasting security certainty level of cloud and on-premise systems, more than half (38 of 74 respondents) concurred that on-premise systems and conventional server farms were more secure than open cloud. The figure was less than anticipated, as the significant lion's share of writing audited in this research concurred that cloud adds greater security risks and threats because users must address both customary and new, cloud-specific vulnerabilities. At the point when asked about the general population cloud's readiness for mission-basic enterprise applications, the vote was a tie: 34% (25 of 74 respondents) were in assertion, and other 34% were

in disagreement. There was substantial assertion that cloud safety is relied upon to enhance as approximately 75% (55 of 74 respondents) showed that open cloud will be more secure later on as the service models turn out to be more develop and better technologies end up plainly accessible.

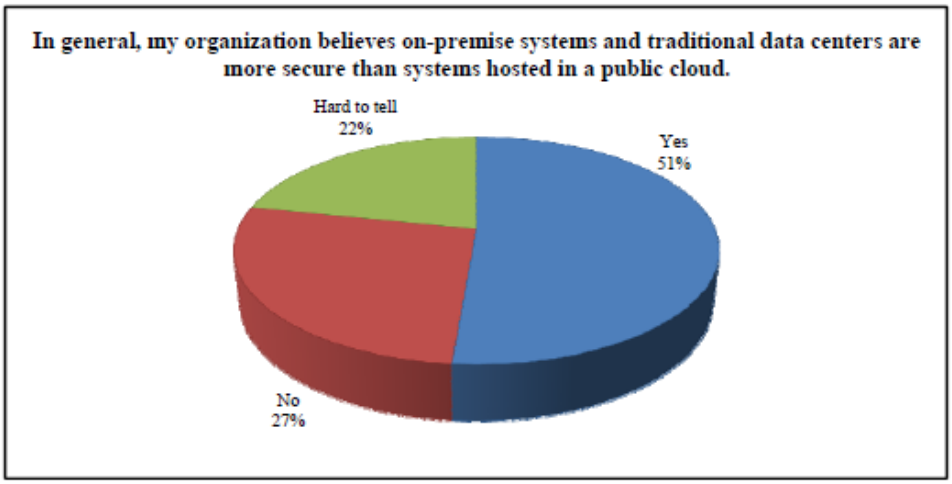

Figure 6 On-premises is more secure than cloud

In the survey, 11 most actively discussed security concerns were presented, and the respondents were asked to rate how each element would affect their organizations' decision making process in cloud adoption in a scale of five:

- No concern (0),
- mild concern (1),
- concern (2),
- serious concern (3),
- and show stopper (4).

Vol. 6 Issue 7, July - 2016

ISSN: 2249-3905 | Impact Factor: 6.573 |Thomson Reuters Researcher ID: L-5236-2015

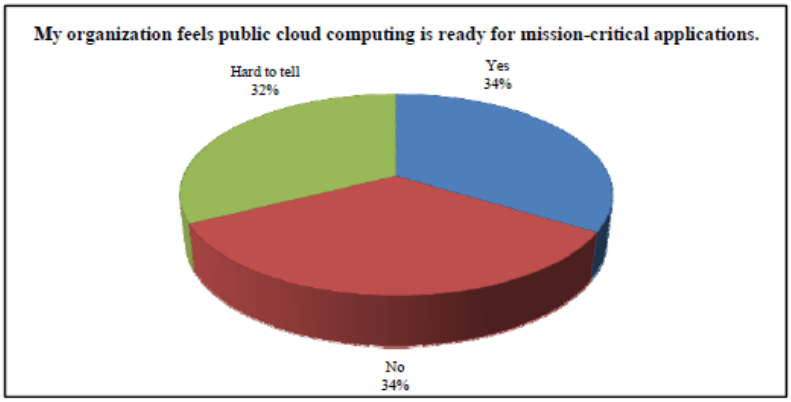

Figure 7 Cloud readinesses for mission-critical applications

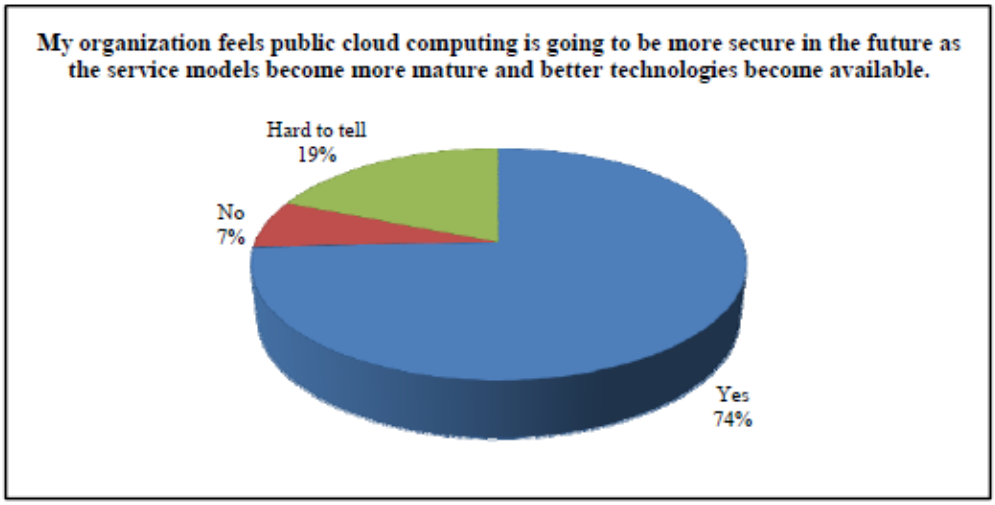

Figure 8 Cloud will be more secure in the future.

The core questions in the survey and descriptive statistics are presented on each question. The conversion method used for Liker scale data is discussed in the previous chapter.

CONCLUSION

The results show that both current and prospective cloud users are well aware of the existing risks and threats, yet the majority of them believe cloud computing is reasonably secure for both non-critical and mission-critical application deployments. Because of the nature of the technology and architecture it is based on, cloud computing does require more preventative measures and broader

security perimeter than traditional, on-premise application and data hosting. However cloud computing, if properly planned and deployed, will bring positive economic, functional, and for some organizations additional security benefits. The favorable outcome is being the primary driving force, as the recent economic fallout is forcing organizations seek more cost effective solutions, and this trend of favoring cost-saving solutions is likely to continue at a rate consistent with the growth of cloud adoption.

REFERENCES

1. Ajey Singh and Dr. ManeeshShrivastava, Overview of Security issues in Cloud Computing, International Journal of Advanced Computer Research (ISSN (print): 2249-7277 ISSN (online): 2277-7970) Volume 2 Number 1March 2012.
2. Anthony Bisong, Syed (Shawon) M. Rahman, An Overview of the Security Concerns in Enterprise Cloud Computing, International Journal of Network Security &Its Applications (IJNSA), Vol.3, No.1, January 2011.
3. Anita Kumari Nanda, Brojo Kishore Mishra," Privacy and Security issues in Cloud Computing", International Journal of Advanced Computer Research (IJACR),Volume-2 Number-4 Issue-6 December-2012.
4. Andrei, T. Cloud Computing Chaleenges and Related Security Issues, p.5. 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 IEEEConference on High Perfomance Computing and Communications. IEEE
6. Berman, S., Kesterson-Townes, K., Marshall, A., &Srivatbsa, R. (2011). The power of cloud: driving business model innovation. [10] CSA (2012). Are enterprises really ready to move into the cloud? Retrieved July 30, 2012, from CSA:https://cloudsecurityalliance.org/wp-
7. Catteddu, D., &Hogben, G. (Eds). November 2009, Cloud computing Risk Assessment, European Network and Information Security Agency (ENISA).
8. Dustin Amrhein, P. A., Andrew De Andrade, Joe, Armstrong, E. A. B.,James Bartlett, Richard Bruklis, Ken Cameron, et al. (2010) Cloud Computing Use Cases White Paper. Version 3.0 ed., Cloud computing Use Case Discussion Group
9. Foster, I., Zhao, Y., Raicu, I., and Lu, S., 2008: Cloud Computing and Grid Computing 360-Degree Compared, 2008 Grid Computing Environment Workshop (GCE '08), November 12-16, 2008, Austin, Texas
10. John Rhoton, "Cloud Computing Explained: Implementation Handbook for Enterprises", 2nd Edition, ISBN 978-0-9563556-0-7, Recursive Press, 2011.
11. Mohammed Al-Zoube, " E-Learning on the Cloud", International Arab Journal of e-Technology, Vol. 1, No. 2, June 2009.
12. Bisong, A. and Rahman, S.S.M. (2011). An Overview of the Security Concerns in Enterprise CloudComputing. International Journal of Network Security & Its Applications, 3(1), 30-45.doi:10.5121/ijnsa.2011.3103.