IJCTA, 9(23), 2016, pp. 211-218

Effective Management of Security of Risk in Cloud Computing Environment

Anil Barnwal* Asit Dwivedi Rajesh Jangade*** and Satyakam Pugla******

Abstract : The different risks of security related with each and every model of cloud delivery may differ and are based on a number of factors such as the importance of information, structure of clouds, security controls used in a specific cloud system. As the times passes on, different organizations give some relaxation in their security. To counter this relaxation, the various security providers perform regular security checkups. This security checkup is an important tool for reducing the threats, overcoming the weaknesses of the system and easing security risks. This paper is used to manage the security risk in the cloud computing environment and also identify various risks and susceptibility. It covers all the models of cloud service and deployment. Then the provider of cloud can apply it to various organizations to perform mitigation of risk.

Keywords : LOB, PaaS, SaaS, IaaS, ESB, CSP, SLA

1. INTRODUCTION

The advantages of cloud computing are well known and there is necessity to build suitable and efficient security system for implementation of cloud. In spite of the normal challenges of developing secured information technology systems, sometimes cloud computing systems provides an extra level of risk because its important services are outsourced by third party. These outsourcing sometimes makes it difficult for maintaining integrity and privacy of data, supporting availability of various data and services and reveal various agreements [1]. A survey is conducted by IDC to measure the opinions and the enterprise use of information technology services by the various information technology executives and their business oriented coworkers, shown in figure 1. In today's environment security has become a biggest challenge and sensitive issue for cloud computing [2].

The various risks related to the cloud computing are quite old today and it can be obtained from various organizations. The properly planned various risk management activities will be important to indicate that information is simultaneously available as well as protected [3]. If methodologies of risk management is planned and organized properly then it helps the management to control and provide the essential security measures.

The atmosphere of Cloud computing which is available in the various formats and models have different ways to justify the various susceptibility and threats to an organization. This paper provides an important environment for better understanding of the organizational security. The services of Cloud can be useful to this environment in the organizations for mitigation of risk.

* Amity University, Noida, U.P. abarnwal@amity.edu
** Amity University, Noida, U.P. asitdwivedi@rediffmail.com
*** Amity University, Noida, U.P. rjangade@amity.edu
**** Amity University, Noida, U.P. spugla@amity.edu

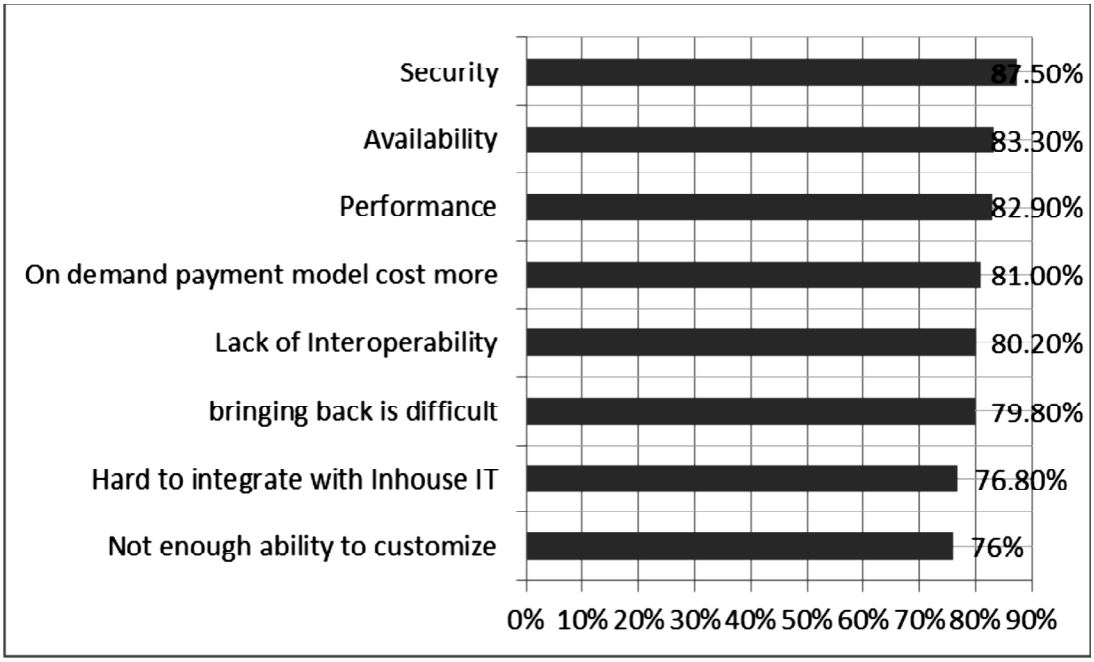

Fig. 1. Cloud Servey Model couducted by IDC.

2. DIFFERENT ISSUES OF SECURITY IN CLOUD COMPUTING ENVIRONMENT

Cloud computing utilize the three types of delivery model to provide services to the different end users. These models include PaaS, SaaS and IaaS respectively, providing resources for infrastructure, software for services and platform based application to the users. These models provide various level of security requirement in cloud computing. The architecture of cloud computing has IaaS at it lower level upon which PaaS is placed and the top level containing SaaS. Practically as the capacities are acquired, so are the security issues related to data and the diverse dangers. There are numerous noteworthy exchange offs to every model in the terms of coordinated components, tensility versus intricacy and security. On the off chance that the cloud administration supplier deals with just the security at the base level of the security design, then the purchasers turn out to be more responsible for executing and dealing with the security capacities. According to the review [4] conducted by the Cloud Security Alliance (CSA) and IEEE that the customers across various sectors are ready to adopt the cloud based computing but major concern is related to its security. Hence the provider needs to ensure the rapid increase in its cloud security and its related drivers. The increasing demand of cloud computing not only shows how cloud computing is starting a new trend in computing and reshaping the IT sector, but also shows how lack of a consistence domain is having adverse effect on its growth.

2.1. SaaS Related Security Issues

In cloud computing models such as SaaS, the user using the cloud platform are dependent on the provider for providing them with reliable security measures. The provider of cloud services must be fully aware to ensure and prevent different users across the cloud to access each other's data. Hence it is difficult for user to be aware of as security measures are setup properly. Furthermore, it's difficult to assure the application used will be available in future when needed [5].The cloud user in SaaS by default will be replacing the old application software's with new ones. In this way the attention is not on versatility of utilization, but rather to stabilize or improve the pre-existing security given by the legacy application and accomplishing an effective way to ensure the migration of data [6].The SaaS software developer and merchant can host these application on its own personal servers or on a distributed cloud computing infrastructure maintained by an outside suppliers such as third-party like google, IBM etc. Using the pay-as-you go approach in cloud computing enables the provider to concentrate and focus on providing reliable services to its user.

During the last few years, computing devices have integrated into various ventures as a result IT services and computing resources has turned into a basic and important asset. Today's Enterprises view information and business methods like evaluating data, records, exchanges, and so on as its crucial and important to protect such data with control to its access and various policies. However in SaaS, the data of one enterprise is stored in the server of provider with data of other business enterprise. If SaaS Provider is utilizing the maximum of public cloud rather than private cloud computing services then there is the probability of enterprise data being stored with other data that is unrelated to the enterprise such as data belonging to SaaS application. Likewise the provider uses multiple cloud servers across the world to store data of enterprise on it to ensure accessibility of data at any moment of time. Since enterprises are aware of SaaS model, however the data still remains accessible within its boundaries with respect to their policies. But there are major concerns regarding the data availability, application threats and threats of data theft which can lead to losses in terms of liabilities and finance.

2.2. Security Issues Related To PaaS

The Provider of PaaS may give some benefit to the general population to construct a few applications on its platform. Still the security provided beneath the level of application will be under the control of provider and it's the responsibility of the provider to ensure that data remains blocked between applications. PaaS models are used to provide the developers to develop their own applications using the top layer of PaaS model architecture. This exchange spreads to security highlights and limits, where there is less flexibility in the intrinsic capacities and there is more versatility in the layer on additional security.

Application which are trying to impact ESB also known as Enterprise Service Bus must provide security to ESB specifically, controlling convention such as WS i.e Web service security [7].The PaaS models lack the ability to divide the ESB, to ensure the efficiency of programs related to security application Metrics must be used, enumerating and measuring the efficiency of code for application. Consideration must also be given to these malignant programmers respond to latest architecture of PaaS cloud models that stops various components of application from scrutinizing. Sometimes it may happen that hackers might attack on the visible codes which are running during application execution. There is additionally a chance that they may attack the architecture and undergo performing protracted black box testing. The cloud is not vulnerable only due to its relation with various web applications but also due to the SOA application also known as Service -Oriented Architecture that run from system to system, which are continuously set up at increasing rate on the cloud.

2.3. Security Issues Related To IaaS

Using the IaaS model of cloud architecture developer can have great control over the security as compare to SaaS and PaaS model of cloud architecture, until their exist no loop hole in virtualization manager security. Howsoever, hypothetically virtual machines can address these issues yet in reality there are various security problems [8][9].The other element that affects is the reliability of data which is stored inside the hardware of cloud service provider. With increase in virtualization, the main issue faced is to ensure that the owner of data has full control and access over his data regardless where ever the data is stored among the cloud servers across any geographical location. So to maintain and achieve the ultimate security of data stored on the cloud and develop trust among users for cloud resources various methods must be applied [10]. The responsibilities for security of both provider and the user contrast in cloud services models. For instance EC2 model of Amazon popularly known as the "Elastic Compute Cloud" [11] architecture , Incorporate responsibility of the cloud service provider to ensure updated level of security for VMM *i.e*. Virtual Machine monitor, suggesting that the provider can only relate and solve security issues like virtualization security and environmental security etc, whereas the client user is in charge for various controls of security that pertain to information technology systems incorporating application, storage of data and also operating systems.[6]

3. ANALYZING THE RISK FACTOR WITH DIFFERENT SECURITY SENSITIVITY ISSUE

The various risk types (such as integrity, security, performance and availability) are similar with those cloud systems which do not have proper cloud security solutions. The risk level of an organization generally changes if cloud solutions are adopted (depending on for what purpose and how the cloud solutions are accepted and utilised). This is mainly due to the changes in probability and impact with respect to the events (residua and inherent) of risk associated with the Content security policy (CSP) that has been used for various services.

There are various characteristic risks associated with cloud computing systems. They are:

3.1. Force Of Disruption

According to some organizations innovation facilitation and cost saving through cloud computing, is considered as risk events. Cloud computing could interrupt some of the business models by letting down the entry barriers for new competitors and even make them outdated in the coming future. For example, there is decline in the sale of DVDs (Digital Versatile Discs), CDs (Compact Discs) at different physical stores due to Internet Technology. Currently available competitors who are fully embraced by cloud may bring some new innovations and ideas in the markets quickly to sustain themselves. Since the cloud computing solutions reduces the capital expenditure by yielding the short term shaving, so some organization adopting the cloud might make good margin over its non-cloud competitors. Thus when members of an industry implements a cloud computing solutions, then other organizations could also be forced to follow the same rule and implement the same [12].

3.2. Living In The Ecosystem Of Same Risk As The Content Security Policy(CSP) And Other Residents Of The Cloud

When an enterprises implements cloud computing solutions managed by third party then some trust relationship in coordination with CSP are formed with respect to the risk universe, legal liability, incident response, incident escalation and some other areas. These activities of the CSP and their cloud residents can influence the business in various ways. Let us consider the below mentioned points:

Generally, providers of the third party cloud service and their client organizations are different enterprises but if the CSP unable to fulfill its responsibilities then it may have some authorized liability implications for different CSP's client organizations. But if a client of cloud organization unable to fulfill it responsibilities then there is less chance of any legal implications to the CSP.

Providers of cloud service with their client groups have different programs of ERM (Enterprise Risk management) to define all the areas of supposed risk. In few cases that involve many high dollar yielding contracts, CSPs will try to integrate their ERM programs with their associated clients. The bunch of risks opposing an organization that uses cloud computing of third party contains a part risks that is faced by CSPs and risks faced by an individual [13].

3.3. Lack Of Transparency

A CSP hardly disclose the detailed information about it operations, processes, methodologies and controls. For example, clients of cloud have to look into the data storage locations, algorithms used by the CSP to allocate different computing resources, how client data is separated within cloud and the specific controls used to protect components of the cloud computing architecture.

3.4. Issue Of Performance And Reliability

System failure that can occur in a computing environment is a risk event but it offers unique challenge in the environment of cloud computing. Although a service level agreement is defined to meet specific requirements but CSP solutions sometimes not able to fulfill these performance metrics due to some un-expected demands.

3.5. Absence Of Interoperability Or Portability Of Application Among Users

Content Security policies provide some tools of software development along with their cloud solutions. If these development tools are exclusive, then they may create some applications that work only within the solution boundaries of different CSPs. Subsequently these new applications, which are created exclusively, may not work well with systems that do not lie in the boundary of the cloud solutions. Furthermore, the more number of applications developed with these exclusive tools and the more organizational data stored in the cloud solutions of the CSPs, it will become more difficult to change providers.

3.6. Issues Of Security And Compliance

Based on what different processes supported by cloud computing, some security and retention issues may come up to comply with the laws and regulations such as the Health Insurance Portability and Accountability Act of 1996 and the Acts of Sarbanes-Oxley of 2002 and the different data privacy and protection laws endorsed in various countries. Examples of these data privacy and protection regulations would include IT Amendments of India, Personal Data Protection Act 2010 of Malaysia, the Patriot Act of USA and the Data Protection Directive of EU. Depending on the different cloud solutions used (PaaS, IaaS and SaaS), an organization of cloud client may not obtain and review security incident or operations on network as they are in the control of CSP. The Content security policy might not disclose this information or might not do anything without ignoring the privacy of other clients using the cloud infrastructure.

3.7. More Number Of Cyber-Attack

The Association of a number of administrations operating on infrastructure of a CSP presents more attractive targets than a single organization, thus increasing the chances of attacks. Furthermore the risk levels of CSP solutions are higher compared to data integrity and confidentiality.

3.8. Data Leakage Risk

In multi-client cloud environment where resources are shared between enterprises and applications, presents data leakage risks that may not exist if resources and dedicated servers are used exclusively by a single organization. This data leakage risk presents an extra point of consideration with respect to meeting confidentiality and data privacy requirements.

3.9. Organizational Changes In Information Technology

If cloud computing is implemented at a higher scale then an organization require less number of internal information technology personnel in the areas of development of application, deployment of technology , management of infrastructure and maintenance. The result of this would be the risk of losing dedication and morale of the remaining IT staff.

3.10. Sustainability Of Cloud Service Provider

In today's world many companies are new in providing cloud services or even for existing companies also business of cloud computing is a new one. So the projected profitability and longevity of cloud service is not known. Hence some CSPs are reducing the offering of cloud service because they are not much profitable from business point of view. Result of this would be facing the operational disruptions or loss of time and expenses of searching and adopting some alternate solutions, for example returning back to in house presented solutions.

3.11.

Apart from these risks, there are some other features of cloud computing that may generate some lesser known challenges that warrant evaluation. Management teams may be interested to accept the risks of running the whole organization in a public cloud given the small direct capital investment requirements. Start-up and venture investors may sometimes prefer to focus their investments on the business models irrespective of the technology

infrastructure that would be of very limited value if the venture were about to fail. Start-ups can organize their business models with the help of cloud solutions more easily and economically as compared to last generation technology options. All the risks of cloud computing discussed above should undergo a risk assessment test and should be given mindful consideration to prevent from some undesirable consequences. Many risks discussed above are not likely to be modified by clauses of contractual with a CSP. Furthermore some modified and upgraded solutions may be required to be implemented beyond the instant cloud solutions provided with the help of CSP.

4. RISK MANAGEMENT AND SECURITY SENSITIVITY ISSUE

Risk can be broadly classified into four categories such as Accepting Risk, Transferring Risk, Avoiding Risk and Mitigating Risk. The result of risk analysis is shown in figure 2.

4.1. Accepting Risk

Here Risk is accepted unconditionally. Risk here depends on external factors like laws. Although the actions taken here to counteract with these threats are indirect things which depend on same external factors, so it is upto the system to accept the given condition or change the constraint.

4.2. Transferring Risk

Here risk is transferred to third party. Although the problems here are supposed to come from a Cloud service provider, so the risks are generally transferred. The action taken against such threats are under observation of third party but it is guaranteed by the service provider itself.

4.3. Avoiding Risk

Here risks are avoided and some alternatives are shown. The risks here are generally identified by the cloud service providers and cloud users. So the actions taken to tackle these threats are grouped into two categories: the situation where the user required to be adjusted or the situation when the Cloud service provider takes some actions to tackle such problems. So an extreme and difficult countermeasure is required.

4.4. Mitigating Risk

Here Risk is decreased to the level at which it is accepted. Risks which are grouped into Mitigation of Risk are likely to include regulatory agreement of the different Cloud service provider, its description, verification, etc. It was then checked whether the standard of the Cloud service provider is adjusted, or it develops according to the standard of the Cloud service provider to handle the risk generated in the system.

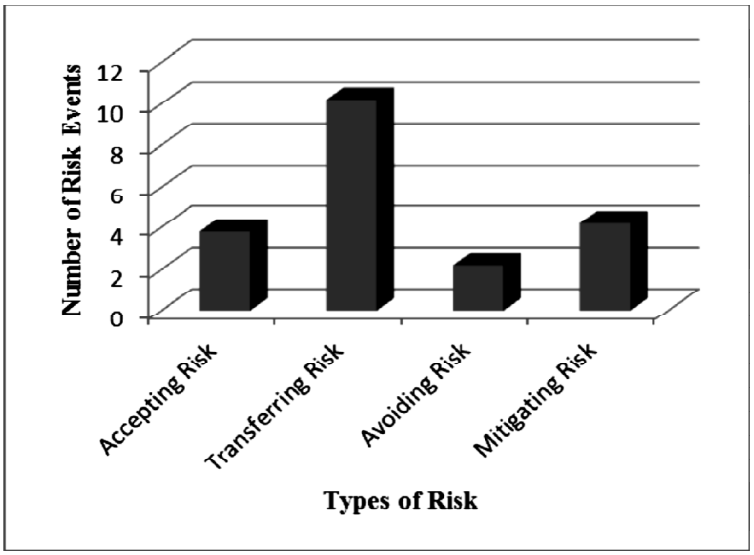

Fig. 2. Result of Risk Analysis

5. RESULT AND DISCUSSION

Transfer of computing load gives a chance to ease the various difficulties, cost and capital expenditure in the system. So the real advantages of cloud computing are cost cutting and balance through volume of operations, charging according to the usage of data, a higher and more speed in the market by introducing data components and outsourcing less important activities like capacity planning and scalability

Forming a self-service information technology and cost cutting may be very effective but it may sometimes worth nothing.

However service level agreements (SLAs) can sort out some problems that arise in the system, but the real problems can be finally sorted out only when the clients actually switch between the providers of their choice in the real world. Although this happens in many organizations and this switching created a competitive environment in the market place. Until that kind of markets established completely, organizations may use their home made solutions because they have invested huge amount of capital in the market which is spread across the product world.

Although the proper marketing of the functions of the cloud and its services are not done, still it is believed that cloud will capture the market because of its low cost, low maintenance, quality of its services and hassle-free switching between providers. In these situations, problems related to supply of services may also be removed.

Although the uses and advantages of cloud computing is well known but there are some problems related to the outsourcing of some activities and other risks appears because of temporary changes [14] made in the system.

So before moving to the cloud the most important factor that we should keep in our mind to know our group, know the various solutions of the cloud and its provider. The decision of moving to the cloud should comprise of minimum number of organizational designer, IT leadership, product vendors, developers,, and hiring teams for outsourcing. This may cause sometimes lack of funds in the organizations. While exploring new development in cloud computing it needs adventurous approach and technical intelligence and if group members are not interested to learn new things then it will be discouraging for the organization. Sometimes some group members may think that implementing new approach and developments may lose their job, so it should be dealt properly in the organization.

It may be possible that some managers afraid of shifting towards cloud solutions for job insecurity. Though this reason is valid but it cannot be ignored. Solutions are getting superior day by day and a number of examples are available for its successful implementations [15].

6. CONCLUSION AND FUTURE SCOPE

In this paper Cloud computing security problems have been analyzed in details on the basis of the method of risk breakdown structure and the methods of risk. Furthermore to satisfy extracted risks countermeasures were developed individually. We have also tried delicate the balance between advantages of using cloud computing and various risk factors associated with it. That means, it is supposed that the cloud services provider can improve the vague insecurity of the user by the proposed countermeasure of this paper. Effectiveness of the proposed countermeasure will be evaluated quantitatively in the future. Furthermore the aim of this paper is to improve the objectivity and develop those ideas into specific proposals.

7. REFERENCES

1. Axel Buecker, Koos Lodewijkx, Harold Moss, Kevin Skapinetz, Michael Waidner, “Cloud Security Guidance IBM Recommendations for the Implementation of Cloud Security,” IBM Corp. 2009, p. 7-19.
2. John W. Rittinghouse, James F. Ransome, “Cloud Computing Implement, Management, and Security,” p 153
3. ISACA, “Cloud Computing: Business Benefits with Security, Governance and Assurance Perspectives,” An ISACA Emerging Technology White Paper, pp 7.
4. Cloud Security Alliance, “CSA Cloud Security Alliance Security Guidance for Critical Areas of Focus in Cloud Computing V2.1,” 2009, p. 3068.

5. Choudhary V. Software as a service: implications for investment in software development. In: International conference on system sciences, 2007, p. 209.

6. Seccombe A, Hutton A, Meisel A, Windel A, Mohammed A, Licciardi A, et al. Security guidance for critical areas of focus in cloud computing, v2.1. CloudSecurityAlliance, 2009, p 25.

7. Oracle.WiringthroughanEnterpriseServiceBus,2009 http://www.oracle.com/technology/tech/soa/ mastering-soa-series/ part2.htmlS [accessed on:19February 2010].

8. Attanasio CR. Virtual machines and data security. In: Proceedings of the workshop on virtual computer systems. New York, NY, USA: ACM; 1973. p. 206–9.

9. Gajek S, Liao L, Schwenk J. Breaking and fixing the inline approach. In: SWS '07, Proceedings of the ACM workshop on secure web services. New York, NY, USA: ACM; 2007. p. 37–43.

10. Descher M, Masser P, Feilhauer T, Tjoa AM, Huemer D. Retaining data control to the client in infrastructure clouds. In: International conference on availability, reliability and security, ARES '09, 2009, p. 9–16.

11. Amazon.AmazonElasticComputeCloud(EC2),2010 /http://www.amazon.com/ec2/S[accessed:10 December 2009].

12. Carl Almond, "A Practical Guide to Cloud Computing Security What you need to know now about your business and cloud security," Avanade Inc., August 2009, p. 6-27.

13. Babu M.S., Babu A.M., Sekhar M.C., Enterprise Risk management Integrated framework for Cloud computing. In International Journal of Advanced Networking and Applications, 2013, p.1939-1950

14. Ubuntu, "An Introduction to Cloud Computing," pp. 5.

15. Maria Spinola, "An Essential Guide to Possibilities and Risks of Cloud Computing," June 2009, p. 12.