ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 2, March 2016

AN ANALYSIS OF SECURITY ISSUES AND CHALLENGES IN CLOUD COMPUTING

R. Angeline.A.P.(OG)
Department of Computer Science and Engineering,
SRM University,Ramapuram Campus
BharthiSalai, Ramapuram,
Chennai-089, Tamil Nadu

J. Caroline El Fiorenza.A.P.(OG)
Department of Computer Science and Engineering,
SRM University,Ramapuram Campus
BharthiSalai, Ramapuram,
Chennai-089, Tamil Nadu

D.Devahema.A.P.(OG)
Department of Computer Science and Engineering,
SRM University,Ramapuram Campus
BharthiSalai, Ramapuram,
Chennai-089, Tamil Nadu

ABSTRACT

Cloud computing is a set of IT services that are provided to a customer over a network on a leased basis and with the ability to scale up or down their service requirements. Usually cloud computing services are delivered by a third party provider who owns the infrastructure. It advantages to mention but a few include scalability, resilience, flexibility, efficiency and outsourcing non-core activities. Cloud computing offers an innovative business model for organizations to adopt IT serviceswithout upfront investment.

It provides people the way to share distributed resources and services that belong to different organization. Since cloud computing uses distributed resources in open environment, thus it is important to provide the security and trust to share the data for developing cloud computing applications.

This paper show how we secure the cloud security, privacy and reliability when a third party is processing sensitive data. In this paper, we have discussed security risks and concerns in cloud computing and enlightened steps that an enterprise can take to reduce security risks and protect their resources. This paper introduces a detailed analysis of the cloud computing security issues and challenges focusing on the cloud computing

This paper also tackles the important aspect of security concerned challenges which the researchers and authors are facing in the security of cloud computing.

1. INTRODUCTION

Cloud computing is currently one the most hyped IT innovations. Most IT companies announce to plan or (suddenly) already have IT products according to the cloud computing paradigm. Though cloud computing itself is still not yet mature enough, it is already evident that its most critical flaw in security [1][2]. In the nearest future, we can expect to see a lot of new security exploitation events around cloud computing providers and users, which will shape the cloud computing security research directions for the next decade. Hence, we have seen a rapid evolution of a cloud computing security discipline, with ongoing efforts to cope with the idiosyncratic requirements and capabilities regarding privacy and security issues that this new paradigm raises. In this development, we closely watch cloud computing security on a very technical level, focusing primarily on attacks and hacking attempts related to cloud computing providers and systems. We pointed out lately, the specific security threats and vulnerabilities of services and service-oriented architectures require new

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 2, March 2016

security criteria, so do attacks on cloud computing scenarios. In this work-in-progress paper, we try to anticipate the classes of security issues that will arise from the cloud computing paradigm.

II. CLOUD COMPUTING ARCHITECTURE

There are several major cloud computing providers including Amazon, Google, Sales force, Yahoo, Microsoft and others that are providing cloud computing services (Figure1. shows current cloud providers).Cloud computing providers provide a variety of services to the customers and these services include e-mails, storage, software-as-a-services, infrastructure-as-a-services etc.

Figure-1 Cloud Computing Architecture

Service Models:

Cloud Software as a Service (SaaS). The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Cloud Platform as a Service (PaaS). The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.

Cloud Infrastructure as a Service (IaaS). The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

III. ISSUES IN CLOUD

Security is the most important issue in cloud computing. We are residing everything in providers premises which makes the information highly unsecured [6]. It's a main obstacle in adoption of cloud computing. According to the IDC's survey on the cloud services, security concerns are number one issue facing cloud computing [7][8]. IDC's findings in the survey of 224 IT executives are shown in fig.2. Difficulties or overheads in front of cloud computing are the danger of-Disrupts Services, Theft of Information, Loss of Privacy, Damage of information. These problems prevent the organizations to adopt

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 2, March 2016

whereas the Microsoft Word templates are self-contained. Causal Productions has used its best efforts to ensure that the templates have the same appearance.

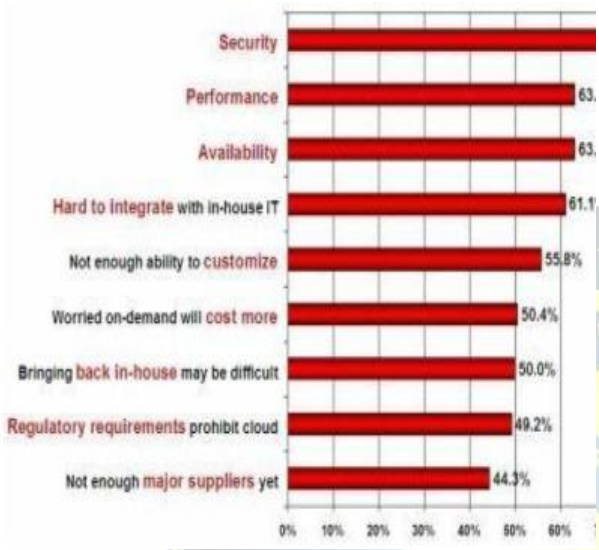

Figure 2. Analysis of major issues of cloud computing

III. THREATS IN CLOUD COMPUTING

Cloud computing faces just as much security threats that are currently found in the existing computing platforms, networks, intranets, internets in enterprises. These threats, risk vulnerabilities come in various forms The Cloud Security Alliance (Cloud Computing Alliance, 2010) did a research on the threats facing cloud computing and it identified the *flowing major threats:*

- Failures in Provider Security
- Attacks by Other Customers
- Availability and Reliability Issues
- Legal and Regulatory Issues
- Perimeter Security Model Broken
- Integrating Provider and Customer Security Systems
- Insecure Application Programming Interfaces
- Malicious Insiders
- Shared Technology Vulnerabilities
- Data Loss/Leakage
- Account, Service & Traffic Hijacking

IV CLOUD COMPUTING CHALLENGES

The current adoption of cloud computing is associated with numerous challenges because users are still skeptical about its authenticity. Based on a survey conducted by IDC in 2008, the major challenges that prevent Cloud Computing from being adopted are recognized by organizations are as follows:

A. Security: It is clear that the security issuehas played the most important role in hindering Cloud computing acceptance. Without doubt, putting your data, running your software on someone else's hard disk using someone else's CPU appears daunting to many. Well-known security issues such as data loss, phishing, botnet (running remotely on a collection of machines) pose serious threats to organization's data and software. Moreover, the multi-tenancy model and the pooled computing resources in cloud computing has introduced new security challenges that require novel techniques to tackle with. For example, hackers can use Cloud to organize botnet as Cloud often provides more reliable infrastructure services at a relatively cheaper price for them to start an attack.[9]

B. **Costing Model:** Cloud consumers mustconsider the tradeoffs amongst computation, communication, and

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 2, March 2016

integration.

This problem is particularly prominent if the consumer uses the hybrid cloud deployment model where the organization's data is distributed amongst a number of public/private (in-house IT infrastructure)/community clouds. Intuitively, ondemand computing makes sense only for CPU intensive jobs.[9].

C. Charging Model: The elastic resourcepool has made the cost analysis a lot more complicated than regular data centers, which often calculates their cost based on consumptions of static computing. Moreover, an instantiated virtual machine has become the unit of cost analysis rather than the underlying physical server. For SaaS cloud providers, the cost of developing multitenancy within their offering can be very substantial. These include: re-design and redevelopment of the software that was originally used for single-tenancy, cost of providing new features that allow for intensive customization, performance and security enhancement for concurrent user access, and dealing with complexities induced by the above changes. Consequently, SaaS providers need to weigh up the trade-off between the provision of multitenancy and the cost-savings yielded by multi-tenancy such as reduced overhead through amortization, reduced number of on-site software licenses, etc. Therefore, a strategic and viable charging model for SaaS provider is crucial for the profitability and sustainability of SaaS cloud providers.[9]

V. SOLUTION OF SECURITY ISSUES

Find Key Cloud Provider First solution isof finding the right cloud provider. Different vendors have different cloud IT security and data management. A cloud vendor should be well established, have experience, standards and regulation. So there is not any chance of cloud vendor closing.

Clear Contract Contract with cloud vendorshould be clear. So if cloud vendor closes before contract, enterprise can claim.

Recovery Facilities Cloud vendors shouldprovide very good recovery facilities. So, if data are fragmented or lost due to certain issues, they can be recovered and continuity of data can be managed.

Better Enterprise Infrastructure Enterprisemust have infrastructure which facilitates installation and configuration of hardware components such as firewalls, routers, servers, proxy servers and software such as operating system, thin clients, etc. Also should have infrastructure which prevents from cyber-attacks.

Use of Data Encryption for security purpose Developers should develop theapplication which provides encrypted data for the security. So additional security from enterprise is not required and all security

VI. CONCLUSION

Cloud computing is a combination of several key technologies that have evolved and matured over the years. Cloud computing has a potential for cost savings to the enterprises but the security risk are also enormous. Enterprise looking into cloud computing technology as a way to cut down on cost and increase profitability should seriously analyze the security risk of cloud computing. The strength of cloud computing in information risk management is the ability to manage risk more effectively from a centralize point. 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.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 2, March 2016

However, one must be very careful to understand the security risks and challenges posed in utilizing these technologies. Cloud computing is no exception. In this paper key security considerations and challenges which are currently faced in the Cloud computing are highlighted. This paper also analyze cloud computing vulnerabilities, security threats cloud computing faces and presented the security objective that need to be achieved. On one hand, the security-sensitive applications of a Cloud computing require high degree of security on the other hand, cloud computing are inherently vulnerable to security attacks. Therefore, there is a need to make them more secure and robust to adapt to the demanding requirements of these networks.

REFERENCES

[1] Ricardo vilaca, Rui oliveira 2009. Clouder: A Flexible Large Scale Decentralized Object Store. Architecture Overview. Proceeding of WDDDM '09

[2] Michael Miller. 2009. Cloud Computing-Web Based Application that change the way you collaborate online. Publishing of QUE, 2nd print.

[3] National Institute Of Standard and technology. csrc.nist.gov/groups/ SNS/cloud-computing/cloud-def-v15.doc, 2009

[4] Open Security Architecture http://www.opensecurityarchitecture.org/

[5] Tim Mather, Subra Kumaraswamy, Shahed Latif Cloud Security and Privacy : An Enterprise perspective of Risks

[6] GregBoss, Padma Malladi, Dennis Quan, Linda Legregni and Harold hall 2007. Cloud Computing. Available from www.ibm.com/developerworks/websphere/zones/hipods/.

[7] Anthony T.Velte, Toby J.Velte and Robert Elsenpeter 2010. Cloud Computing-A Practical Approach. Publishing of Tata McGRAW Hil.

[8] Nils Gruschka and Meiko Jensen, "Attack Surfaces: A Taxonomy for Attacks Cloud Services". IEEE rd International Confrence on Cloud Computing,2010.

[9] Buyya R, Chee Shin Y, Venugopal S, Broberg J, Brandic I. Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing as the 5th utility. Future Generation Computer Systems; 2009; 25(6):599–616.

[10] Armbrust M, Fox A, Griffith R, Joseph A D, Katz R, Konwinski A, Lee G, Patterson D, Rabkin A, Stoica I, Zaharia M. A View of Cloud Computing. Communications of the ACM ; 2010; 53(4):50–58.

[11] Subashini S, Kavitha V. A survey on security i ssues in service delivery models of cloud computing. Journal of Network and mputer Applications; 2011; 4(1):1–11.

[12] Takabi H, Joshi J B D, Ahn G. Security a nd privacy challenges in cloud computing environments. IEEE Security & Privacy;2010;8(6) :24–31.

[13] Sangroya A, Kumar S, Dhok J, Varma V. Towards analyz ing data security risks in cloud computing environments.

Communications in Computer and Information Science; 2010; 54 :255–265.

[14] Boss G, Malladi P, Quan D, Legre gni L, Hall H. Cloud computing, 2009. h ttp://www.ibm.com/developerswork/websph ere /zones/hipods/ library.html.

[15] Peter Mell, Timothy Grance. The NIST Definition of Cloud Computing (Draft). NIST. 2011. http://www.production scale.com/home/2011/8/7/the-nist-efinition-of-cloud computingdraft.html#axzz1X0xKZRuf.