



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

A Survey Paper on Cloud Security Issues and Challenges

Pankaj Singhai¹, Prof. Saurabh Sharma²

¹Research Scholar, Dept. of Computer Science, Gyan Ganga College of Technology, Jabalpur, Madhya Pradesh, India

²Assistant Professor, Dept. of Computer Science, Gyan Ganga College of Technology, Jabalpur,
Madhya Pradesh, India

ABSTRACT: Cloud computing is the product of the fusion of traditional computing technology and network technology like grid computing, distributed computing parallel computing and so on. It aims to construct a perfect system with powerful computing capability through a large number of relatively low-cost computing entity, and using the advanced business models like SaaS (Software as a Service), PaaS (Platform as a Service), IaaS (Infrastructure as a Service) to distribute the powerful computing capacity to end users' hands. This article introduces the background and service model of cloud computing. This article also introduces the existing issues in cloud computing such as security, privacy, reliability and so on. Proposition of solution for these issues has been provided also.

KEYWORDS: cloud computing; security; privacy; issue

I. INTRODUCTION

Cloud computing is not a total new concept; it is originated from the earlier large-scale distributed computing technology. However, it will be a subversion technology and cloud computing will be the third revolution in the IT industry, which represent the development trend of the IT industry from hardware to software, software to services, distributed service to centralized service. Cloud computing is also a new mode of business computing, it will be widely used in the near future. The core concept of cloud computing is reducing the processing burden on the users' terminal by constantly improving the handling ability of the "cloud", eventually simplify the users' terminal to a simple input and output devices, and busk in the powerful computing capacity of the cloud on-demand. All of this is available through a simple Internet connection using a standard browser or other connection [2]. However, there still exist many problems in cloud computing today, a recent survey shows that data security and privacy risks have become the primary concern for people to shift to cloud computing [3].

II. WHAT IS CLOUD COMPUTING

"Cloud" is a virtualized pool of computing resources. It can:

- Manage a variety of different workloads, including the batch of back-end operations and user-oriented interactive applications.
- Rapidly deploy and increase workload by speedy providing physical machines or virtual machines.
- Support for redundancy, self-healing and highly scalable programming model, so that workload can be recover from a variety of inevitable hardware/software failure
- Real-time monitor resources usage, rebalance the allocation of resources when needed [4].



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

B. Service Model

- Software-as-a-Service (SaaS): Software as a service is software that is deployed over the internet and/or is deployed to run behind a firewall in your local area network or personal computer. This is a “pay-as-you-go” model and was initially widely deployed for sales force automation and Customer Relationship Management (CRM).
- Platform-as-a-Service (PaaS): Platform as a service, another SAAS, this kind of cloud computing provide development environment as a service. You can use the middleman’s equipment to develop your own program and deliver it to the users through Internet and servers.
- Infrastructure-as-a-Service (IaaS): Infrastructure as a service delivers a platform virtualization environment as a service. Rather than purchasing servers, software, data center space or network equipment, clients instead buy those resources as a fully outsourced service.
- Hardware-as-a-Service (HaaS): According to Nicholas Carr [5], “the idea of buying IT hardware or even an entire data center as a pay-as-you-go subscription service that scales up or down to meet your needs. But as a result of rapid advances in hardware virtualization, IT automation, and usage metering and pricing, I think the concept of hardware-as-a-service, let’s call it HaaS, and may at last be ready for prime time.” This model is advantageous to the enterprise users, since they do not need to invest in building and managing data centers.

C. Deployment Model

- Public cloud: In public clouds, multiple customers share the computing resources provided by a single service provider, Customers can quickly access these resources, and only pay for the operating resources. Although the public cloud has compelling advantages, there existing the hidden danger 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. It’s generally deployed in the enterprise’s data center and managed by internal personnel or service provider. The main advantage of this model is that the security, compliance and QoS are under the control of the enterprises.[6]
- Hybrid cloud: A third type can be hybrid cloud that is typical combination of public and private cloud. It enables the enterprise to running state-steady workload in the private cloud, and asking the public cloud for intensive computing resources when peak workload occurs, then return if no longer needed [7].
- Community cloud: Several organizations jointly construct and share the same cloud infrastructure as well as policies, requirements, values, and concerns. The cloud community forms into a degree of economic scalability and democratic equilibrium. The cloud infrastructure could be hosted by a third-party vendor or within one of the organizations in the community.

III. CLOUD COMPUTING ISSUES

In the last few years, cloud computing has grown from being a promising business concept to one of the fastest growing segments of the IT industry. Now, recession-hit companies are increasingly realizing that simply by tapping into the cloud they can gain fast access to best-of-breed business applications or drastically boost their infrastructure resources, all at negligible cost. But as more and more information on individuals and companies is placed in the cloud, concerns are beginning to grow about just how safe an environment it is.



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirce.com

Vol. 5, Issue 5, May 2017

A. Security

Where is your data more secure, on your local hard driver or on high security servers in the cloud? Some argue that customer data is more secure when managed internally, while others argue that cloud providers have a strong incentive to maintain trust and as such employ a higher level of security. However, in the cloud, your data will be distributed over these individual computers regardless of where your base repository of data is ultimately stored. Industrious hackers can invade virtually any server, and there are the statistics that show that one-third of breaches result from stolen or lost laptops and other devices and from employees' accidentally exposing data on the Internet, with nearly 16 percent due to insider theft [8].

B. Privacy

Different from the traditional computing model, cloud computing utilizes the virtual computing technology, users' personal data may be scattered in various virtual data center rather than stay in the same physical location, even across the national borders, at this time, data privacy protection will face the controversy of different legal systems. On the other hand, users may leak hidden information when they accessing cloud computing services. Attackers can analyze the critical task depend on the computing task submitted by the users [9].

C. Reliability

Servers in the cloud have the same problems as your own resident servers. The cloud servers also experience downtimes and slowdowns, what the difference is that users have a higher dependent on cloud service provider (CSP) in the model of cloud computing. There is a big difference in the CSP's service model, once you select a particular CSP, you may be locked-in, thus bring a potential business secure risk.

D. Legal Issues

Regardless of efforts to bring into line the lawful situation, as of 2009, supplier such as Amazon Web Services provide to major markets by developing restricted road and rail network and letting users to choose "availability zones" [10]. On the other hand, worries stick with safety measures and confidentiality from individual all the way through legislative levels.

E. Open Standard

Open standards are critical to the growth of cloud computing. Most cloud providers expose APIs which are typically well-documented but also unique to their implementation and thus not interoperable. Some vendors have adopted others' APIs [11] and there are a number of open standards under development, including the OGF's Open Cloud Computing Interface. The Open Cloud Consortium (OCC) [12] is working to develop consensus on early cloud computing standards and practices.

F. Compliance

Numerous regulations pertain to the storage and use of data require regular reporting and audit trails, cloud providers must enable their customers to comply appropriately with these regulations. Managing Compliance and Security for Cloud Computing, provides insight on how a top-down view of all IT resources within a cloud-based location can deliver a stronger management and enforcement of compliance policies. In addition to the requirements to which customers are subject, the data centers maintained by cloud providers may also be subject to compliance requirements [13].



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirce.com

Vol. 5, Issue 5, May 2017

G. Freedom

Cloud computing does not allow users to physically possess the storage of the data, leaving the data storage and control in the hands of cloud providers. Customers will contend that this is pretty fundamental and affords them the ability to retain their own copies of data in a form that retains their freedom of choice and protects them against certain issues out of their control whilst realizing the tremendous benefits cloud computing can bring [14].

H. Long-term Viability

You should be sure that the data you put into the cloud will never become invalid even your cloud computing provider go broke or get acquired and swallowed up by a larger company. "Ask potential providers how you would get your data back and if it would be in a format that you could import into a replacement application," Gartner says [15].

I. Solution

To advance cloud computing, the community must take proactive measures to ensure security. The solution is the data encryption. Before storing it at virtual location, encrypt the data with your own keys and make sure that a vendor is ready for security certifications and external audits. Identity management, access control, reporting of security incidents, personnel and physical layer management should be evaluated before you select a CSP. And you should minimize personal information sent to and stored in the cloud. CSP should maximize the user control and provide feedback. Organizations need to run applications and data transfer in their own private cloud and then transmute it into public cloud. While there are many legal issues exist in the cloud computing, Cloud Security Alliance should design relevant standards as quickly as possible.

IV. CONCLUSION

In this paper, we discuss a new technology: cloud computing. Describe its definition and some existing issues. There is no doubt that the cloud computing is the development trend in the future. Cloud computing brings us the approximately infinite computing capability, good scalability, service on-demand and so on, also challenges at security, privacy, legal issues and so on. To welcome the coming cloud computing era, solving the existing issues becomes utmost urgency!

REFERENCES

- [1] http://en.wikipedia.org/wiki/Cloud_computing.
- [2] Rich Maggiani, solari communication. "Cloud computing is changing how we communicate".
- [3] Randolph Barr, Qualys Inc, "How to gain comfort in losing control to the cloud".
- [4] Greg Boss, Padma Malladi, Dennis Quan, Linda Legregni, Harold Hall, HiPODS, www.ibm.com/developerworks/websphere/zones/hipods/
- [5] <http://www.rougthtype.com>.
- [6] Tharam Dillon, Chen Wu, Elizabeth Chang, 2010 24th IEEE International Conference on Advanced Information Networking and Applications, "Cloud computing: issues and challenges".
- [7] June 13,2009, <http://server.zol.com.cn/183/1830464.html>.
- [8] Elinor Mills, January 27,2009. "Cloud computing security forecast: clear skies".
- [9] Jianchun Jiang, Weiping Wen, "Information security issues in cloud computing environment", Netinfo Security,doi:10.3969/j.issn.1671-1122.2010.02.026.
- [10] C. Clark, K. Fraser, S. Hand, J. G. Hansen, E. Jul, C. Limpach, I. Pratt, and A. Warfield, [2005] "Live migration of virtual machines" In Proc. Of NSDI'05, pages 273-286, Berkeley CA, USA, 2005. USENIX Association.
- [11] Eucalyptus Completes Amazon Web Services Specs with Latest Release. [12] Open Cloud Consortium.org.
- [13] July 27,2009. Available from <http://fx.caixun.com/>.
- [14] Jack Schofield. Wednesday 17 June 2009 22.00 BST, <http://www.guardian.co.uk/technology/2009/jun/17/cloud-computing-jack-schofield>.
- [15] Gartner. "Seven cloud-computing security risks". <http://www.infoworld.com> July 02,2008.