IOSR Journal of Computer Engineering (IOSRJCE)
ISSN: 2278-0661 Volume 3, Issue 1 (July-Aug. 2012), PP 40-43
www.iosrjournals.org

An Overview on Security Issues in Cloud Computing

Dr. Balachandra[1], D N Kartheek[2]
[1](Dept of I&CT, MIT, Manipal University, INDIA,
[2](Dept of CSE, SVEC, INDIA,

Abstract : *Cloud Computing, a rapidly developing information technology has aroused the concern of the whole world. Cloud Computing is Internet-based computing, whereby shared resources, software and information are provided to computers and devices on-demand, like the electricity grid [1]. 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 capability to end the users' hands. This paper introduces the background and service model of cloud computing. This paper also introduces the existing issues in cloud computing such as security, privacy, reliability and so on.*

Keywords:- *Cloud Computing, Service Models, Security, Privacy.*

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 services to centralized service. 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].

Cloud computing is a model for enabling convenient and on demand network access to a shared group of computing resources that can be rapidly released with minimal management effort or service provider interaction. Cloud has advantages in offering more scalable, fault-tolerant services with even higher performance. Also, Cloud computing can be referred to as a new kind of storage technology, by which we can share software, data or documents to computers as well as other devices on demand.

Cloud Service providers (CSP) (e.g. Microsoft, Google, Amazon, Salesforce.com, GoGrid) are leveraging virtualization technologies combined with self-service capabilities for computing resources via the Internet. In these service provider environments, virtual machines from multiple organizations have to be co-located on the same physical server in order to maximize the efficiencies of virtualization. Cloud service providers must learn from the managed service provider (MSP) model and ensure that their customers' applications and data are secure if they hope to retain their customer base and competitiveness. Today, enterprises are looking toward cloud computing horizons to expand their on-premises infrastructure, but most cannot afford the risk of compromising the security of their applications and data.

International Data Corporation (IDC) conducted a survey (see Fig.1.) of 263 IT executives and their line-of-business colleagues to gauge their opinions and understand their companies' use of IT cloud services. Security ranked first as the greatest challenge or issue of cloud computing.

Fig.1. Results of IDC ranking security challenges.

Corporations and individuals are concerned about how security and compliance integrity can be maintained in this new environment. Even more concerning, though, is the corporations that are jumping to the cloud computing while being oblivious to the applications of putting critical applications and data in the cloud. Moving critical applications and sensitive data to a public and shared cloud environment is a major concern for corporations that are moving beyond their data centers' network perimeter defense. To alleviate these concerns, a cloud solution provider must ensure that customers can continue to have the same security and privacy controls over their applications and services, provide evidence to these customers that their organization and customers are secure and they can meet their Service level agreements and show how can they prove compliance to their auditors.

II. What Is Cloud Computing

A. Definition

"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 [3].
- ✓

Fig: Visual Model of Cloud Computing Definition.

B. Service Models

Three types of models exist for providing services of cloud. These three models are often referred to as the **SPI Model** (Software, Platform and Infrastructure) [4].

- ✓ **Software as a Service (SaaS):** Customers obtain the facility to access and use an application or service that is hosted in the cloud. As an example 'Salesforce.com', where necessary information for the interaction between the customer and the service is hosted as part of the service in the cloud.
- ✓ **Platform as a Service (PaaS):** Customers obtain access to the platforms by enabling them to organize their own software and applications in the cloud.
- ✓ **Infrastructure as a Service (IaaS):** The facility provided to the customer is to lease processing, storage and other fundamental computing resources. The customer does not manage or control the basic cloud infrastructure but has control over operating systems, storage, deployed applications.

C. Deployment Models

In spite of the delivery models utilized, there are three primary ways in which cloud services can also deployed and are described.

- ✓ **Public Cloud:** In public cloud, customers can access web applications and services over the internet. Each individual customer has its own resources which are dynamically provided by a third party vendor (cloud providers). These providers facilitate multiple customers from multiple data centers, manage all the security measures and provide hardware and infrastructure for the cloud customers to operate. The customer has no idea about how the cloud is managed or what infrastructure is available. Customers of public cloud services are considered to be untrusted.
- ✓ **Private Cloud:** In private clouds customers has complete control over that how data is managed and what security measures are in place while data processing in cloud.
- ✓ **Hybrid Cloud:** Hybrid Clouds are a combination of public and private clouds within the same network. Private cloud customers can store personal information over their private cloud and use the public cloud for handling large amount of processing demands.
- ✓ **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.

D. Characteristics

Cloud Computing has a wide range of characteristics some of which are as follows:

- ✓ **Shared Infrastructure:** Cloud environment uses an effective software model that allows sharing of physical services, storage and networking capabilities among users. The cloud infrastructure is to find out most of the available infrastructure across multiple users.
- ✓ **Network Access:** Cloud Services are accesses over a network from a wide range of devices such as PCs, laptops and mobile devices by using standards based APIs.
- ✓ **Handle Metering:** Cloud service providers store information of their clients for managing and optimizing the service and to provide reporting and billing information. Due to this, customers are payable for services according to how much have actually used during the billing period.

E. Architecture

Cloud architecture, the systems architecture of the software systems involved in the delivery of cloud computing, typically involves multiple cloud components communicating with each other over a loose coupling mechanism such as a messaging queue. Elastic provision implies intelligence in the use of tight or loose coupling as applied to mechanisms such as these and others.

III. Security Issues In Cloud Computing

Cloud Computing is a model for information and services by using existing technologies. It uses the internet infrastructure to allow communication between client side and server side services/applications [5]. Cloud Service Providers (CSP's) exist between clients that offer cloud platforms for their customers to use and create their own web services.

When making decisions to adopt cloud services, privacy or security has always been a major issue. To deal with these issues, the cloud provider must build up sufficient controls to provide such level of security than the organization would have if the cloud were not used. The majoy security challenge is that the owner of the data has no control on their data processing. Due to involvement of many technologies including networks, databases, operating systems, resource scheduling, transaction management, concurrency control and memory management [6], various security issues arises in cloud computing.

A. Security

Where is your data more secure, on your local hard drive 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 inside theft [7].

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 depending on the computing task submitted by the users [8].

C. Reliability

Servers in the cloud have the same problem 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 abig 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. Open Standard

Open Standard are critical to the growth of cloud computing. Most cloud prividers expose APIs which are typically well-documented but also unique to their implementation and thus not interoperable. Some vendors have adopted others APIs [9] and there are a number of open standards under development, including the OGF's

Open Cloud Computing Interface. The Open Cloud Consortium (OCC) [10] is working to develop consensus on early cloud computing standards and practices.

E. 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 appropiately with these regulations. Managing complaince 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 complaince policies. In addition to the requirements to which customers are subject, the data centers maintained by cloud providers may also be subject to complaince requirements [11].

F. 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 [12].

IV. Conclusion

Cloud Computing became a buzzword nowadays. More and more companies step into cloud and provide services above on it. However, security and privacy issues impose strong barrier for users' adoption of cloud systems and cloud services. There is no doubt that the cloud computing is the development trend in the future. Cloud computing brings us the approximately infinite computing capabilities, good scalability, service on-demand and so on, also challenges at security, privacy, reliability and so on. More security strategies should be deployed in the cloud environment to achieve the 5 goals i.e. availability, confidentiality, data integrity, control and audit, as well as privacy acts should be changed to adapt a new relationship between users and providers in the cloud literature. We claim that prosperity in Cloud Computing literature is to be coming after those security and privacy issues are resolved.

References

[1] http://en.wikipedia.org/wiki/Cloud_computing.
[2] Rich Maggiani, solari communication, "Cloud computing is changing how we communicate".
[3] GregBoss,PadmaMalladi,DennisQuan,LindsLegregni, HoroldHall,HiPODS,www.ibm.com/developerworks/websphere/zones/hipods/
[4] "Security Guidance for critical areas of Focus in Cloud Computing", April 2009, presented by Cloud Security Alliance (CSA).
[5] Kevin Curran, Sean Carlin and Mervyn Adams "Security issues in Cloud Computing", published in August 2011, Elixir Network Engg. (www.elixirjournal.org).
[6] Kevin Hemalen, Murat Kantarciouglu, Latifur Khan and Bhavani Thuraisingham, The University of Texas at Dallas, USA, "Security Issues for cloud computing", April-June 2010, international journal of information security and privacy.
[7] Elinor Mills, January 27,2009. "Cloud computing security forecast: clear skies".
[8] Jianchun jiang, Weiping Wen, "Information Seucirty issues in cloud computing environment", Netinfo security,doi:10.3969/j.issn.1671-1122.2010.02.026.
[9] Eucalyptus Completes Amazon Web Services Specs with Latest Release.
[10] OpenCloudComputing.org.
[11] http://fx.caixum.com/.
[12] Gartner, "Seven cloud-computing security risks". http://www.infoworld.com.