ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 10, October 2015

Study of Threats and Security in Cloud Computing Technology

Vinayak D. Shinde[1], Anas Dange[2], Muhib Anwar Lambay[3]

H.O.D., Department of Computer Engineering, Shree L.R. Tiwari College of Engineering, Mira Road, Mumbai, India [1]

Lecturer, Department of Information Technology, Theem College of Engineering, Boisar, Mumbai, India [2]

Assistant Professor, Department of Computer Engineering, Theem College of Engineering, Boisar, Mumbai, India [3]

Abstract: Cloud computing plays a vital role in the service of internet by providing the facility of virtually infinite computing resources on-demand and eliminating the need of hardware and software infrastructure. The advantages of virtualizing applications are eminent: minimizing the cost of hardware, reducing the need to buy software license, decreasing the implementation cost as client pays only for what is needed and globalizing the workforce which improves the accessibility there by increasing the efficiency. This support has led to the evolution of many new cloud initiatives, ranging from private clouds to the well-known publicly accessible clouds such as Google, Amazon, etc. Cloud computing is not just of what computing service is delivered but how it is being delivered is equally important. In spite of its indispensable benefits, there are certain critical challenges that need to be taken care of before going in for this technology. On one hand, the untrusted cloud servers are not entitled to access the outsourced data content for data secrecy, and on the other hand, the data resources are not physically under the full control of data owner. In this paper, we analyse the various security threats and vulnerabilities involved in cloud computing which will help us to upgrade the benefits of cloud computing. Finally, this paper discusses some solutions to secure the information of an enterprise for cloud computing deployment.

Keywords: cloud computing, virtualization, service of internet, security threats.

I. INTRODUCTION

The concept of internet started evolving when J.C.R. Licklider, in 1960s, introduced the term "intergalactic computer network" at the Advanced Research Projects Agency [1]. After the concept of TCP/IP was standardized, the Internet was introduced in 1982. It is a network of networks that consists of hundreds of private, public, and government networks, the scope of whose ranges from local to global and is linked by a wide range of electronic, wired, optical and wireless networking technologies. Internet started to make huge impact on world with electronic mail, instant messaging, video calls, social networking, blogs, online shopping sites and discussion forums. Nowadays, increasing amount of data is being transmitted at high speeds due to networking developments like fibre optics. In the year 1993, only 1% of information flowed through two-way telecommunication networks which increased to 57% by 2000 and 97% by 2007 [2]. All these technological innovations led to the development new business model which is cloud computing.

II. CLOUD COMPUTING

Today, most of the information technology journals, magazines and websites are talking about cloud computing in one way or the other. This technology has been evolving since 1961 when John MacCharty suggested in a speech at MIT that computing can be sold like a utility, just like water or electricity [3] and its use has multiplied since last decade. But, what is cloud computing? Cloud computing (CC), is a new concept that has the goal to make computational resources available as services on demand, in a short period of time and usage based cost. The services provided like storage, processing etc. are operated with the help of web servers known as 'cloud 'and the GUI which is imparted by the customer's browser. However, The National Institute of Standards and Technology; or NIST, an agency of the U.S. Department of Commerce which was founded in 1901; and whose mission is to promote the nation's innovation and technology in science, has defined cloud computing as: "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

Salesforce.com came into being in 1999 and became the first website to deliver business applications from a 'normal' website, which is now known as cloud computing [4]. In 2002, Amazon Web Services launched a suite of cloud-based services, including storage, computation, and even human intelligence through the Amazon Mechanical Turk. Later in 2006, Amazon expanded its cloud services with Elastic Compute cloud (EC2), allowing people to access computers and run their own applications on them via the cloud. Today, the latest example of cloud computing is Web 2.0; Google, Yahoo, Microsoft, and other service providers.

Based on the levels at which resources can be shared, the variants of cloud computing can be depicted as: an

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 10, October 2015

infrastructure cloud (for example, hardware or IT infrastructure management), a software cloud (for software, middleware, or customer relationship management as a service), an application cloud (application, UML modelling tools, or social networks as a service), and a business cloud (i.e., business processes as a service)

Thus the advantages of cloud computing place it as the best solution for traditional computing difficulties and complexities, but the technical experts share many concerns about cloud computing environment, in particular, data security being the most significant one. Surveys conducted by the IDC Enterprise Panel in 2008 and 2009 showed that CIOs consider confidentiality, availability, and reliability as primary concerns [5]. Similarly, 70 per cent of respondents in a survey from Japan specified their concerns on the security in cloud computing [6]. In addition, the European Network and Information Security Agency (ENISA) conducted a survey of small and medium-sized business, which confirmed that, their major concern on cloud computing included data confidentiality and liability for incidents that involved the infrastructure [5, 7]. Hence, Cloud service providers and users, regardless of their size, may fall victim to one or more security breaches at some point of time. It's therefore of little surprise that cloud security and privacy are growing as a striking area of analysis for researchers.

This paper firstly gives information about characteristics of cloud computing, then mentions different security threats involved in cloud computing and finally talks about the recommendations to mitigate the security threats.

III. CLOUD COMPUTING – SERVICE MODELS

For clouds, there exist three principal service models: software as a service (SaaS), in which applications are hosted by a cloud service provider and made available to customers over internet; platform as a service (PaaS), in which programming platform is created for the programmer to develop, test, run and manage the applications and infrastructure as a service (IaaS), wherein the customer organization outsources its IT infrastructure such as servers, networking, processing, storage, virtual machines and other resources. Thus, we can summarize these models as: SaaS, where the consumer controls only the application configurations; PaaS, where consumers can control only the hosting environment and IaaS, where the consumer controls everything except the data center infrastructure.

IV. CLOUD COMPUTING – DEPLOYMENT MODELS

Cloud computing also has four main deployment models; Public model which allows the accessibility of systems and services easily to general public like amazon, Google, etc.; Private model which allows the accessibility of systems and services within the particular organization and managed either internally or a third party; Community model where the cloud's infrastructure is exclusively used by a specific community of consumers and Hybrid clouds that can be formed by combining two or more of the other cloud computing models.

V. CHARACTERISTICS OF CLOUD COMPUTING

Cloud computing offers several key characteristics. NIST has mentioned five key features of cloud computing; resource pooling, wide network access, on demand self-service, rapid elasticity, and measured service. [8]

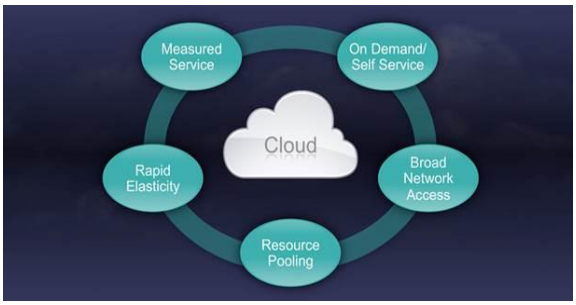

Fig. 1: Essential characteristics of cloud computing

A. *On-demand self-service*

A cloud computing user has provision of independently modifying computing capabilities as needed automatically without requiring the human interaction with individual service provider.

B. *Resource pooling*

The cloud provider's computing resources like storage; processing, memory, etc. are pooled together to serve the needs of multiple consumers with various different virtual resources dynamically assigned and reassigned to meet the consumer's demands. Also, there is a location transparency in which the customer has no knowledge of the exact location of the provided resources.

C. *Broad network access*

The cloud computing service is accessible by any network-based appliance; which can be less powerful; such as desktop, laptop, smart-phone and tablet device. Generally, the customer use the web browsers to access the cloud services.

D. *Rapid elasticity*

The cloud computing capabilities can be elastically expanded or reduced by the cloud service provider according to the consumers' requirements. . To the consumer, these capabilities appear to be unlimited and this operation might be done automatically and efficiently.

E. *Measured service*

The consumers pay only for the exact amount of resources, which they have utilized. Hence, the Resource usage can be monitored and reported, there by providing transparency to both the consumer and provider of the utilized service.

F. *Virtualization*

Virtualization is a technique of running multiple operating systems or applications on a unique physical hardware at the same time. Virtualization differs from cloud

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 10, October 2015

computing because virtualization is software that manipulates hardware, while cloud computing refers to a service that is a result obtained from that manipulation. Cloud computing can exist without virtualization; however, most of the cloud projects are developed using virtualization technology.

G. Multi-tenancy

Tenants access a pool of resource; reserve some resources for their operations and then release them when they finished. [9]

VI. THREATS IN CLOUD COMPUTING

If the cloud computing provider whose vulnerabilities are easiest to exploit is identified by the cybercriminal, then this entity becomes a highly visible target [2]. Thus, the lack of security related with this single provider threatens the entire cloud in which it resides. Being a combination of several technologies, cloud computing technology has wide variety of risks associated with it; some of which are discussed below:

A. Physical Security:

At first data must be secured physically. The importance of Physical security is often underestimated in support of more technical and dramatic issues like hacking, viruses, Trojans, and spyware. However, these attacks can be carried out with slight or no technical knowledge. Moreover, this not only includes penetrations by intruders, but also protection against natural calamities and disasters such as floods, and human errors, which are part of our day-today life and are inescapable.

B. Data Location:

Most of the cloud service providers have their data centers spread across the globe. So, in some cases, these applications and data might be stored in countries, which can have judiciary concerns or data might not be accessible because of laws of the country. Hence cloud computing customers often prefer providers in their own country for legal processes since they have sensitive personal data or private data.

C. Misuse of Cloud:

One of the greatest benefits of cloud computing is that it offers customers the access to vast amount of computations, often coupled with a weak registration process where anyone can register and immediately start using cloud services. However, not everyone uses this power for good purpose. The attacker might use an array of cloud servers to crack an encryption key within few minutes which might have taken months or years to crack using his own limited hardware. PaaS providers have already suffered most from these kinds of attacks; however, recent study shows that hackers have started targeting IaaS vendors as well.

D. Data Segregation:

The data of various different customers are stored in the same devices of the cloud computing providers. Poor segregation of resources may increase the risk of vulnerability. Attackers might succeed in stealing the data saved on the same machine. If the design and modelling of multitenant cloud database is not proper, a bug in an application of one client could allow an attacker to access not only the data of that client, but every other client's details as well. This threat can be solved by providing strong encryption to the cloud data which may in turn affect the customers in a way that the available data might not be correctly sent to the customer whenever required.

E. Account Hijacking:

Account hijacking is not a new concept. Attackers can steal the credentials and using this; can often access the biting areas of deployed cloud computing services. Simple Internet registration systems, phishing and fraud schemes allow a hacker to take full control of the account. In the month of April 2010, Amazon came across a Cross-Site Scripting (XSS) bug which allowed the attackers to steal the credentials from the site.

F. Data Loss:

Since the infrastructure and computational resources are shared, the cloud service provider's should have powerful authentication systems that grant access to data. Of course, data stored in the cloud can also be lost due to reasons other than malicious attackers; like any accidental deletion by the provider, or even worse, a physical catastrophe such as a fire or earthquake. Backup measures should be in place to avoid this kind of data loss. In 2012 summer, the attackers broke into the Gmail and Twitter accounts of Mat Honan, writer of Wired magazine and used this access to erase all his personal data in those accounts.

G. Data Recovery Threat:

The cloud characteristics of pooling of resources states that the resources allocated to one user may be reallocated to other user at a later time. Therefore, for storage resources, it might be possible that the following user may recover the data written by earlier user.

H. Insecure Interfaces:

Cloud computing providers expose a set of Application programming interfaces (API) that are used by the customers to establish, manage, interact and monitor the cloud services. The security of these interfaces against accidental and malicious attempts reflects the security of general cloud services. Furthermore, in some cases; these interfaces are developed by third parties to offer the services which add value to their customers, which in turn increases the risk related to confidentiality, integrity and accountability.

I. Malicious Insiders:

CERN defines an insider threat as such: [10]

"A malicious insider threat to an organization is a current or former employee, who has or had authorized access to an organization's network, system, or data and intentionally misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information."

DOI 10.17148/IJARCCE.2015.41008

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 10, October 2015

The organizations may be at risk since they doesn't need to know about the technical details of the delivery of the services. A provider may not reveal its process and procedures, how it grants access to physical assets, monitoring of employees, and compliance related issues to the customer.

J. Internet Protocol Vulnerabilities:

The characteristic of cloud computing states that the cloud services are accessed via standard protocols network, which in most cases, is the Internet. Thus all the threats related to data transfer - such as vulnerabilities that allow spoofing or MIM (man-in-the-middle) attacks or leakage in the network - are therefore relevant for cloud computing [11]. Hence the data must be encrypted whenever transferred.

VII. SECURITY IN CLOUD COMPUTING

Cloud computing security is an evolving sub-domain of computer security, network security, and, more broadly, the information and data security. It refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and those associated with cloud computing use.

When starting to use cloud computing, consumers must have a clear idea of potential security benefits and risks related to cloud computing, and set genuine outlooks with their cloud provider. Additionally, this paper emphasis on the role that standards play to improve cloud security and also identifies areas where future standardization could be effective.

It also provides an overview of the security and privacy challenges applicable to cloud computing and points out attention that organizations should evaluate when outsourcing data, applications, and infrastructure to a cloud computing environment.

A. Cloud Security Guidance

As consumers move their applications and data to the cloud in order to use this technology, it is very important that the level of security provided in the cloud environment should at least be equal to or more efficient than their own traditional IT environment. Failure to ensure suitable security protection can result in the huge loss of business thus wiping out the fruitful impact of cloud computing.

B. Cloud Security Implementation Steps

1. Selection of the correct application for Public Cloud.

Some business organizations with new start-ups begin by making use of public cloud for their applications. We cannot use public clouds for every organization. Enterprise applications suitable for the public cloud aren't subject to severe security requirements. In this case Websites, application development, and testing and online product files use the security given by most cloud service providers (CSPs) is more suitable for these kinds of applications.

2. Analysis of CSP's Security.

CSPs provide many levels of public cloud security and also provide guidelines for examining information security risks, keeping in mind the threats, vulnerabilities and impacts, for the designing and implementation of information security systems, and for making use of the management processes to ensure that these guidelines are followed. Organizations considering taking sensitive programs and data to the public cloud may workout and compare various CSPs depending upon the standards.

3. Identification of the Right Third-Party Services.

When comes to security agreement, organizations can not simply go as per the CSP's statement. Many third-party services can audit the actual, application of security standards, processes at a CSP and compare them with those promised to the client.

4. Addition of Authentication Layers.

Most of the CSPs provide a very good authentication services for public cloud instances. We need to find out the benefits of better public cloud security against the costs of increased network latency. If one wishes to apply their own encryption instead of, or in addition to, those provided by the CSP, then many installable packages can do this type of encryption on the fly.

5. Placement of Security in-front of the SLA.

When you run a private cloud, you should have the tools to know when and where security gaps occur. Public cloud security guarantee with CSP's are not good enough unless and until they are noted as service level agreements in the contract, If there are transparent monitoring and reporting functions available to the cloud customer, then the agreement itself may be fruitless.

6. Transparent Security Processes.

The need for transparent security processes, procedures and practices within your SLA go far away from the potential data gaps. Whenever you go for the hosted servers, they provide a physical facility, and such as a rack and a set of physical servers those you can visit anytime. But in case of the public clouds, you are unaware about the exact physical location of your cloud server, in this situation you have to consider the information that is given by the CSP. Thus the transparency is very critical.

7. Organize the Logging and Monitoring processes.

While doing the inspection on the monitoring and logging processes of physical cloud with CSPs, it is necessary to ensure public cloud security. While differentiating one CSP's logging and monitoring activity with another before you sign a SLA, it may give out superior differences in the security that is provided.

8. Connecting with Multiple CSPs.

It is common practice to obtain high-bandwidth network connections which is given to the cloud servers from multiple vendors; this can be followed in order to make aware about the risk of disconnection from many service

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 10, October 2015

providers. When one of them is down, then the other one has a very good opportunity of being available. Many cloud provisioning tools come already integrated with leading CSPs.

VIII. CONCLUSION

Our work aims to make the enterprises aware about the various threats in cloud computing. Since this technology is an association of several technologies, various threats from lower physical level to higher application level are likely to occur. This paper discusses the various challenges faced in cloud computing. As it is rightly said that a coin has two sides, cloud computing provides indispensible benefits on one hand whereas it gives rise to various possible security threats on the other side. So there is an immediate need to secure the clouds more appropriately. Hence, various recommendations are presented that will mitigate these security threats. Also, this paper provides a fundamental step towards the development of secure cloud computing environments.

REFERENCES

[1] Kaufman, Lori M. "Data security in the world of cloud computing." Security & Privacy in IEEE, 2009, paper 7.4, p. 61-64.
[2] Eken, H. "Security threats and solutions in cloud computing.", Internet Security (WorldCIS) in IEEE, 2013, p. 139-143.
[3] http://www.javatpoint.com/history-of-cloud-computing (access: September 26, 2015)
[4] http://www.photoventure.com/ 2013/ 09/ 04 / history – of - cloud - computing/ (access: September 20, 2015)
[5] P. Saripalli and B. Walters, "QUIRC: A Quantitative Impact and Risk Assessment Framework for Cloud Security," Cloud Computing (CLOUD), IEEE 3rd International Conference 2010.
[6] S. Tanimoto, M. Hiramoto, M. Iwashita, H. Sato, and A. Kanai, "Risk Management on the Security Problem in Cloud Computing," in Computers, Networks, Systems and Industrial Engineering (CNSI), First ACIS/JNU International Conference, 2011, p. 147-152.
[7] Y. Chen, V. Paxson, and R. H. Katz, "What's new about cloud computing security?" University of California, Berkeley UCB/EECS, Jan. 5, 2010.
[8] http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf (access: October 1, 2015)
[9] Albakri, S. H., Shanmgam, B Samy, G. N., Idris, N. B., & Ahmed, A. "A case study for the cloud computing security threats in a governmental organization.", Computer, Communications, and Control Technology (I4CT) International Conference, 2014, p. 452-457.
[10] http://www.cert.org/insider_threat/ (access: October 3, 2015)
[11] Grobauer, Bernd, T. Walloschek, and E. Stöcker. "Understanding cloud computing vulnerabilities." Security & privacy in IEEE, 2011, paper 9.2, p. 50-57.