Volume 5, Issue 1, January 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Research on Cloud Computing Security Threats using Data Transmission

Raj Kumar
Sri Guru Tegh Bahadur
Institute of Management and Information Technology
Affiliated to: GGSIPU, Delhi, India

Abstract— Cloud computing is set of resources and services offered through the Internet. Cloud services are delivered from data centers located throughout the world. Cloud computing facilitates its consumers by providing virtual resources via internet. General example of cloud services is Google apps, provided by Google and Microsoft SharePoint. The rapid growth in field of "cloud computing" also increases severe security concerns. Security has remained a constant issue for Open Systems and internet, when we are talking about security cloud really suffers. Lack of security is the only hurdle in wide adoption of cloud computing. Cloud computing is surrounded by many security issues like securing data, and examining the utilization of cloud by the cloud computing vendors. This paper introduces a detailed analysis of the cloud computing security issues and challenges focusing on the cloud computing types and the service delivery types. This paper mainly proposes the core concept of secured cloud computing. It suggests the cloud computing based on separate encryption and decryption services from the storage service. Due to this increasing demand for more clouds there is an ever growing threat of security becoming a major issue. This paper shall look at ways in which security threats can be a danger to cloud computing and how they can be avoided.

Keywords— Security, Security Threats, Secure Cloud Computing, Risk Management

I. INTRODUCTION

The cloud computing becomes the host issue in industry and academia with the rapid development of computer hardware and software. The cloud computing is the result of many factors such as traditional computer technology and communication technology and business mode. It is based on the network and has the format of service for the consumer. The cloud computing system provides the service for the user and has the character of high scalability and reliability.

Cloud computing‖ simply means, Internet computing, generally the internet is seen as collection of clouds; thus the word cloud computing can be defined as utilizing the internet to provide technology enabled services to the people and organizations. Cloud computing enables consumers to access resources online through the internet, from anywhere at any time without worrying about technical/physical management and maintenance issues of the original resources. Besides, Resources of cloud computing are dynamic and scalable. Cloud computing is independent computing it is totally different from grid and utility computing. Google Apps is the
paramount example of Cloud computing, it enables to access services via the browser and deployed on millions of machines.

Nowadays, we have three types of cloud environments: Public, Private, and Hybrid clouds. A public cloud is standard model which providers make several resources, such as applications and storage, available to the public. Public cloud services may be free or not. In public clouds which they are running applications externally by large service providers and offers some benefits over private clouds. Private Cloud refers to internal services of a business that is not available for ordinary people. Essentially Private clouds are a marketing term for an architecture that provides hosted services to particular group of people behind a firewall. Hybrid cloud is an environment that a company provides and controls some resources internally and has some others for public use. Also there is combination of private and public clouds that called Hybrid cloud. In this type, cloud provider has a service that has private cloud part which only accessible by certified staff and protected by firewalls from outside accessing and a public cloud environment which external users can access to it. There are three major types of service in the cloud environment: SaaS, PaaS, and laaS [1]. In cloud, similar to every proposed technology, there are some issues which involved it and one of them is RAS factor. For having good and high performance, cloud provider must meet several management features to ensure improving RAS parameters of its service such as:

- Availability management
- Access control management
- Vulnerability and problem management
- Patch and configuration management
- Countermeasure
- Cloud system using and access monitoring

Cloud computing, so as to deliver a controllable cloud computing services to the governments, enterprises and individuals without the security threat. Unfortunately, there are only limited efforts towards focusing on cloud computing security (cloud security in short) on behalf of operators. It is therefore necessary to conduct a series of technical researches on cloud security from the perspective of operators, while driving the development and introducing it to the industry. This paper presents security problems encountered in cloud computing, and has a research on many technical solutions for cloud security problems

II. CLOUD SECURITY

Cloud computing and web services run on a network structure so they are open to network type attacks. One of these attacks is the distributed denial of service attacks. If a user could hijack a server then the hacker could stop the web services from functioning and demand a ransom to put the services back online. To stop these attacks the use of cookies and limiting users connected to a server all help stop a DDOS attack. Another such attack is the man in the middle attack. If the secure sockets layer (SSL) is incorrectly configured then client and server authentication may not behave as expected therefore leading to man in the middle attacks. It is clear that the security issue has played the most important role in hindering Cloud computing. Without doubt, putting your data, running your software at someone else's hard disk using someone else's CPU appears daunting to many. Well-known security issues such as data loss, phishing, and 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.

2.1 Service Provider Security Issues

The public cloud computing surroundings offered by the cloud supplier and make sure that a cloud computing resolution satisfies organizational security and privacy needs. The cloud supplier to provision the safety controls necessary to safeguard the organization's information and applications, and additionally the proof provided regarding the effectiveness of these controls migrating organizational information and functions into the cloud.

2.2 Privacy

Privacy is the one of the Security issue in cloud computing. Personal information regulations vary across the world and number of restrictions placed by number of countries whether it stored outside of the country. For a cloud service provider, in every jurisdiction a single level of service that is acceptable. Based on contractual commitments data can store within specific countries for privacy regulations, but this is difficult to verify. In case of Private and confidential customer's data rising for the consequences and potential costs of mistakes for companies that handle. But professionals develop the security services and the cloud service privacy practices. An effective assessment strategy must cover data protection, compliance, privacy, identity management, secure operations, and other related security and legal issues.

2.3Securing Data in Transmission

Encryption techniques are used for data in transmission. To provide the protection for data only goes where the customer wants it to go by using authentication and integrity and is not modified in transmission. SSLITLS protocols are used here. In Cloud environment most of the data is not encrypted in the processing time, but to process data, for any application that data must be unencrypted. In a fully homomorphism encryption scheme advance in cryptography, which allows data to be processed without being decrypted. To provide the confidentiality and integrity of data-in-transmission to and from cloud provider by using access controls like authorization, authentication, auditing for using resources, and ensure the availability of the Internet-facing resources at cloud
provider.

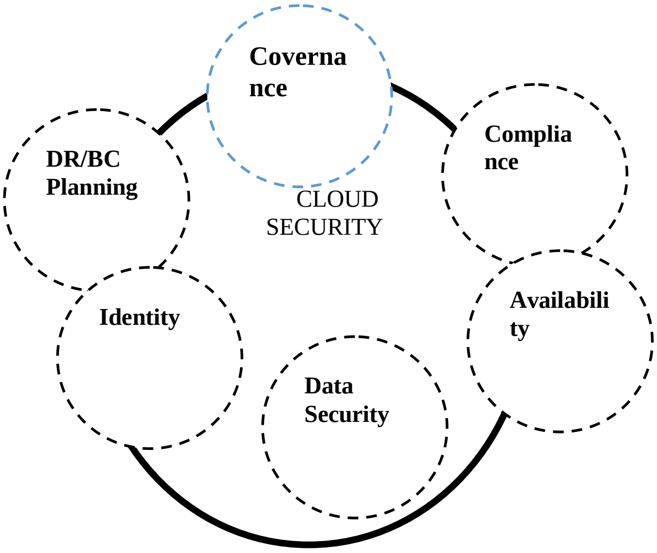

Fig1: Various Point of View of Cloud Security

III. CLOUD SECURITY PROBLEM

The cloud system is running in the internet and the security problems in the internet also can be found in the cloud system. The cloud system is not different the traditional system in the PC and it can meet other special and new security problems. the biggest concerns about cloud computing are security and privacy [9]. The traditional security problems such as security vulnerabilities, virus and hack attack can also make threats to the cloud system and can lead more serious results because of property of cloud computing. Hackers and malicious intruder may hack into cloud accounts and steal sensitive data stored in cloud systems.

The data and business application are stored in the cloud center and the cloud system must protect the resource carefully. Cloud computing is a technology evolution of the widespread adoption of virtualization, service oriented architecture and utility computing. over the Internet and it includes the applications, platform and services. If the systems meet the failure, fast recovery of the resource also is a problem. The cloud systems hide the details of service implementation technology and the management.

The user can't control the progress of deal with the data and the user can't make sure the data security by themselves. The data resource storage and operation and network transform also deals with the cloud system. The key data resource and privacy data are very import for the user. The cloud must provide data control system for the user. The data security audit also can be deployed in the cloud system. Data moving to any authorized place you need it, in a form that any authorized application can use it, by any authorized user, on any authorized device. Data integrity requires that only authorized users can change the data and Confidentiality means that only authorized users can read data.

Cloud computing should provide strong user access control to strengthen the licensing, certification, quarantine and other aspects of data management. In the cloud computing, the cloud provider system has many users in a dynamic response to changing service needs. The users do not know what position the data and do not know which servers are processing the data.

The user do not know what network are transmitting the data because the flexibility and scalability of cloud system. The user can't make sure data privacy operated by the cloud in a confidential way. The cloud system can deploy the cloud center in different area and the data can be stored in different cloud node. The different area has different law so the security management can meet the law risk. Cloud computing service must be improved in legal protection.

IV. PROPOSED WORK

In order to overcome challenges from cloud security, state of- the-art technical solutions relevant to cloud security should be considered. This section shows four typical aspects of technical solutions for operators as shown on Table I.

Security Solution	Description
Continuation Mechansim	The security solution of service migration from non-cloud platform to cloud platform
IDM	Simplified authentication management for cloud environment and end-to-end trustable access technology.
Data security	Data transmission, data isolation, data wiping
virtualization security	Virtualization Machine Monitoring (VMM) security, Virtual Machine (VM) security, and virtualization network security.

A. Continuation of service from traditional platform to cloud platform.

Enterprises are looking to cut costs and gain agility by migrating primary business applications to cloud infrastructure. However, for operators, migrating those applications to cloud infrastructure is proving to be a challenge. Applications are not usually well suited to cloud infrastructure. What's more, managing business workloads in the cloud often requires new IT techniques and brings new risks. Therefore, it is necessary to clarify application migration solutions.

B. Data security

Data Transmission. It is inevitable that data transmission is conducted in cloud computing service. Data transmission security is a common issue not only in non-cloud system, but also in cloud. In order to maintain confidentiality, completeness and availability of network data transmission, encryption schemes, e.g., IPSec, VPN, and SSL are able to be incorporated within cloud computing system. These schemes can provide an encryption channel to cloud computing system.

Data isolation. To implement information separated among cloud users, the scheme like physical isolation, virtualization, and data label can be employed to isolate different customers (tenancy) data and configuration information, so as to protect privacy and security of user data.

Data wiping. Customer's residual data in cloud infrastructure, e.g., disks without data wiping mechanism raises leak of their sensitive information. Therefore, data wiping in cloud is necessary and its steps can be done. Firstly, delete customers' data on the media, e.g., disks in a cloud data center, once the customers have permitted to remove them. Secondly, An inspection should be conducted on these disks, in order to ensure the data has been wiped. Thirdly, the wiped media, e.g., disks then can be redeployed and reused. In case of the disks in which data cannot be wiped, they should be destroyed.

Virtual Firewall. A Virtual Firewall (VF) is a firewall deployed and running entirely within a virtual environment and which provides the packet filtering and monitoring. The VF can be realized in a traditional software firewall on a guest virtual machine already running, or it can be a purpose-built virtual security appliance designed with virtual network security in mind, or it can be a virtual switch with additional security capabilities, or it can be a managed kernel process running within the host VMM.

V. CONCLUSION

In this study different security and privacy related research papers were studied briefly. Cloud services are used by both larger and smaller scale organizations. Advantages of Cloud computing are huge. But it‘s a global phenomenon that everything in this world has advantages as well as disadvantages.Cloud computing is suffering from severe security threats from user point of view, one can say that lack of security is the only worth mentioning disadvantage of cloud computing. Both the Service providers and the clients must work together to ensure safety and security of cloud and data on clouds. Mutual understanding between service providers and users is extremely necessary for providing better cloud security. In this paper we have identified that security is biggest hurdle in wide acceptance of cloud computing. Users of cloud services are in fear of data loss and privacy.

Researchers and IT security professionals must come forward and do more to ensure security and privacy to users. Our study identifies top security concerns of cloud computing, these concerns are Data loss, Leakage of Data, Client‘s trust, User‘s Authentication, Malicious users handling, Wrong usage of Cloud computing and its services .Hijacking of sessions while accessing data. We propose to use The Cloud Security Alliance (CSA) release of a new governance, risk management, and compliance stack for cloud computing. The suite of cloud security tools, available for free download, is meant to help organizations create public and private clouds that comply with industry standards for accepted governance, risk, and compliance (GRC) best practices. The GRC stack has three components: a technical foundation, a controls framework, and a questionnaire for assessing what the CSA calls "industry-accepted ways to document what security.

VI. FUTURE WORK

Cloud computing is not fully mature and still lot needs to be explored. After our current work we are claiming that security is the most important threat to both the users and the vendors of cloud computing. Vendors, Researchers and IT security professionals are working on security issues associated with cloud computing. Different models and tools have been proposed but still nothing fruitful found. While doing research on security

REFERENCES

[1] ss Bowman, S. Roschke, et aI., "Intrusion Detection in the Cloud," presented at the Eighth IEEE International Conference on Dependable, AutonomIc and Secure Computing, Chengdu, China, 2009.

[2] J Brodkin. (2008). Gartner Seven cloud-computinsecurityAvailable:http://www.networkworld.com/news/200S!07020Scloud.html.

[3] D. L. Ponemon, "Security of Cloud Computing Users," 2010.

[4] T. Mather. (2011). Data Leakage Prevention and Cloud Computing. Available: http://www.kpmg.com/Globa1/Pages/default.aspx.

[5] Jinpeng et al, ―Managing Security of Virtual Machine Images in a Cloud Environment‖, CCSW, 2009, Chicago, USA.

[6] Miranda & Siani, ―A Client-Based Privacy Manager for Cloud Computing‖, COMSWARE‘09, 2009, Dublin

[7] N.Brender I. Markov, "Risk perception and risk Management in Cloud Computing:Results from a case study of Swiss Companies", International Journal of Information (2013) 726- 733