Security Problems Analysis Private Cloud Computing Vs. Public Cloud Computing in Giant Organizations

Muhammad Imran Iftikhar
Department of Computer Science
University of Agriculture
Faisalabad, Pakistan

Abdul Aziz Ghazi
Department of Computer Science
Government College University
Faisalabad, Pakistan

Muhammad Irfan Khan
Department of Computer Science
Government College University
Faisalabad, Pakistan

ABSTRACT

Cloud computing is used to manage store and data processing using a remote servers instead of personal computer or local server. It is a general term that used to describe the delivery of hosted services over the internet. In cloud computing user cannot maintain and build their own computing infrastructures and use the computer resource like storage, virtual machine and application as a utility. From previous years, there is lot of advancement in cloud computing. Security of the user data is major issue and most crucial challenge in the cloud computing. Every organization demanded that privacy, integrity and security of data in each operation which is performed on the digital world. The security of the data is explained in the context of secure transformation of the data through the communication networks with cloud computing. For the security of the data from security threats and known attacks some common techniques are used on the database. The main purpose of usage of cloud computing is to make possible quick, secure and convenient data storage and sharing of computing resources on the internet. The aim of analysis is to identify threats and main vulnerabilities in cloud computing.

Keywords

Vulnerabilities, Threats, Cloud Computing, Security Issues, Private Cloud Computing, Public Cloud Computing.

1. INTRODUCTION

Cloud Computing comes in existence thirteen years before with the commencement of Amazon web service. Although the concept of renting service was not new giving cloud computing quite a few antecedents. The idea of cloud computing appear as a utility and is also directly relevant to this progress connected with Grid Computing. It provides number of opportunities and lot of benefits to user by spreading servers all over the world without remarkable investment or with single data centre. It is an innovative technology in terms to run applications and to store data, [1, 2]. Cloud computing is used to manage, store and process data, using a remote servers instead of personal computer or local server [3].

Figure 1 Cloud Computing

Cloud users and cloud providers are basic hubs of cloud computing. The cloud providers like Amazon provides computing resources such as storage, databases and CPU as web services. User can subscribe it when required and can use it on a pay as you go model without prior contracts with cloud providers [2]. The security of cloud computing is closely related to the risk areas like dependency on the public internet, external storage of data, multi-tenancy, integration with internal security of organizations and lack of control [3].
The term threat referred to potential attack on the user resources and data that may lead to misuse of resources or information. The term vulnerability is used to describe the flaws of the system that allows attacks to become successful and it is the probability of asset when it will be unable to resist against the attack of threat. Vulnerability refers to difference between the attacker force and resistance force's ability to resist against the attacker force [6].

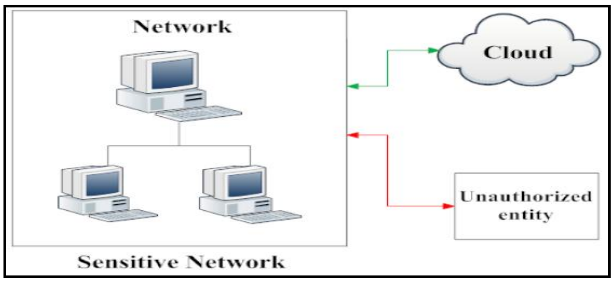

Figure 2 Security Threats to Cloud Computing

1.1 Types of Cloud Computing

The user can get services of the cloud computing like storage, networks, servers, and applications without service provider interaction and with minimal management effort [5]. There are 7 types of cloud computing Private cloud, Public cloud, Hybrid cloud, Community cloud, Distributed cloud, Inter cloud and Multi cloud. In figure 3[Wikipedia] visualizes the cloud computing types and their relationships. Each cloud types offer numerous advantages to the users; the organizations can use more than one type of cloud computing to get maximum advantages [7].

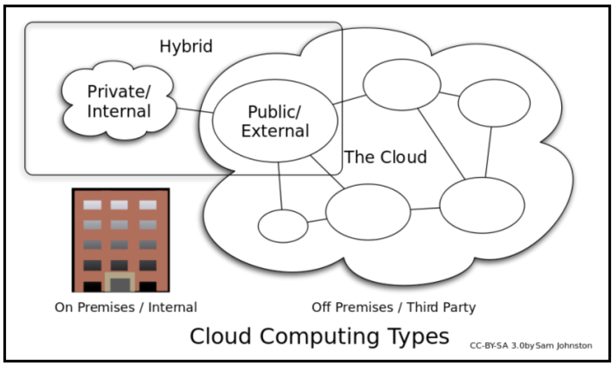

Figure 3 Types of Cloud Computing

1.1.1 Public Cloud

In Public cloud all the resources are available publically, like bandwidth, storage, load balancers and databases by the service provider like Google's App Engine and Amazon Web Services [7]. User can get access to these resources on the basis of pay as you go model or free. It provides the major advantages of cloud computing [8].

1.1.2 Private cloud

The host of the private cloud is the company data centre and these services are only available to the company employees and partners of the company. The main advantage of Private cloud over public cloud is more security of resources and data [7].

1.1.3 Hybrid Cloud

The combination of Public cloud computing and Private cloud computing is known as Hybrid cloud computing. It provides the resources of Public cloud computing with minimal security risk being use of private cloud computing by running highly confidential applications [7, 8].

1.1.4 Community Cloud

The organizations which have commons missions and goals such as policy, security requirements or compliance considerations are used this type of cloud services. The participants shared the cost of cloud services among them. The services of the community cloud are highly secured [7].

1.1.5 Distributed cloud

A Distributed cloud Platform with hub service or single network from different locations of distributed set of machines can be assembled. The types of distributed cloud are volunteer cloud and public resource cloud [11].

1.1.6 Intercloud

It is an extension of the internet and based on the combination of different clouds. We can say it as "cloud of clouds" or "network of networks" [11].

1.1.7 Multicloud

It refers to the use of different cloud computing services in a single heterogeneous architecture, means use of multiple cloud services not a multiple cloud deployment modes [11].

1.2 THREATS IN CLOUD COMPUTING

We can define threat as anything that can cause serious harm or damage our computer system. In the context of computer security a threat is something that may or may not damage but has potential to cause serious harm of computer system. Threats can become the reason of attacks to the security of computer systems and networks. Threats are of different types like Trojans, viruses, hacking etc. Some common types of threats that are related to public cloud computing and private cloud computing are following:

1.2.1 Account or service hijacking:

An account or service can be hijacked through different ways like week credentials and social engineering. If a hacker get access to the user credential than he can use user credential for malicious purposes and can perform malicious activities like manipulate data, access sensitive data etc. It is very old technique to get access to the user data but the methods can be different like fraud, exploitation of software vulnerabilities and phishing. Mostly the passwords and credentials reused which becomes cause of these attacks [10].

1.2.2 Data scavenging

The attacker can recover data through different ways until the device is destroyed. The collection of information from recovered bits of data is known as data scavenging.

1.2.3 Data leakage

During the sharing and storing of data on different resources, the data can be go into wrong hands which can become the reason of data leakage. The data must be secured from unauthorized persons [4].

1.2.4 Denial of Service

The term Denial of Service refers to the situation when intended users have not access to the resources. Due to the malicious user attack it is possible that the service become unavailable when the user post request for resource but the system cannot be satisfy. Normally service becomes unavailable on temporarily basis.

1.2.5 Customer-data manipulation

Customer data manipulation can refer to manipulating the users data which is sent by them from their application component to the server's application.

1.2.6 Virtual Machine (VM) escape

As its name suggested, in virtual machine escape attacker break the system of virtual machine and get access and control to the resources of the host machine [9].

1.2.7 VM hopping

When a malicious user get access to the resources through one VM to another VM on the same physical hardware it is known as VM hopping.

1.2.8 Malicious VM creation

A VM image which has malicious code like Trojan horse can be created by attacker through valid account and attacker can store this malicious code on the provider server. The level of background check of data and privacy laws are different on the basis of geographic area.

1.2.9 Sniffing/Spoofing virtual networks

A malicious user creates malicious VM to gain access when a malicious VM redirect packets of other VMs it is known as Sniffing/Spoofing virtual networks [12].

2. MATERIALS AND METHODOLOGY

Surveys are used as a fundamental gadget which may contain straightforward/close request. The get right outcomes and response, the overviews must be clear, portrayed and brief with respect to the space of the system to be made. Inquiries must focus on the issue. This study was conducted with a sample of 50 IT professionals from multiple service providers & multiple service consumers. The questionnaire which is sent to giant organizations is as follows:

- Do you think that the data stored in the private cloud computing system is safer than public cloud computing?
- Can more troubles occur due to the attacks from known and unknown threats in Private Cloud computing than Public Cloud computing?
- Can more troubles occur due to the attacks hidden inside encrypted traffic in Private Cloud computing than Public Cloud computing?
- Can more troubles occur due to the malware and botnet infection in Private Cloud Computing than Public Cloud computing?
- Can more troubles occur due to the network access to unknown or unauthorized locations in Private Cloud computing than Public Cloud computing?
- Can more troubles occur due to account or service hijacking in Public Cloud Computing than Private Cloud computing?
- Can more troubles occur due to data scavenging in Public Cloud Computing than Private Cloud computing?
- Can more troubles occur due to data leakage in Public Cloud Computing than Private Cloud computing?
- Can more troubles occur due to denial of service in Public Cloud Computing than Private Cloud computing?
- Can more troubles occur due to malicious VM creation in Public Cloud Computing than Private Cloud computing?
- Can more troubles occur due to Sniffing/Spoofing virtual networks in Public Cloud Computing than Private Cloud computing?
- Is Private Cloud Computing more suitable on security basis than Public Cloud Computing for giant scale enterprises?

3. ANALYSIS

The respondents IT specialist were neutral and provide correct information according to their knowledge so we can say the study and analysis of the survey was correct and solid on the basis of collected data and information. We concluded the result of our survey in the form of table and figure in our paper.

Table:1 Comparison of security issues in public and private cloud computing

Security Issues	Private Cloud Computing	Public Cloud Computing
Safety of data	✓	
service hijacking	✓	
data scavenging		✓
data leakage		✓
denial of service		✓
malicious VM creation		✓
sniffing/Spoofing virtual networks		✓
known and unknown threats	✓	
attacks hidden inside encrypted traffic	✓	
malware and botnet infection	✓	
network access to unknown or unauthorized locations	✓	
Malware Injection		✓
Customer-data manipulation		✓
VM roll back attack		✓

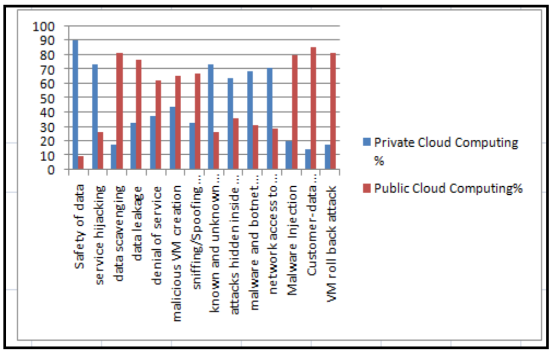

Figure 4 Comparison of security issues in Public and Private Cloud Computing

According to our findings we analyzed that main security issues in Private cloud computing are attacks from unknown and known threats, attacks hidden inside encrypted traffic, botnet and malware infections and unauthorized and unknown locations access to network and in Public Cloud computing main security issues are service or account hijacking, data scavenging, data leakage, denial of service, malicious VM creation and VM migration. The result according to our finding was that the Private Cloud Computing is safer than Public Cloud Computing in giant organizations. On the reliability and security of the data basis the Private Cloud Computing is more reliable and secure than Public Cloud Computing in giant organizations. The most essential finding is that the Private Cloud Computing is perfect and safer for giant scale enterprises, it is all that valuable for giant scale enterprises to adopt Private cloud computing.

4. CONCLUSION

Our research work was survey based, in which we designed a questionnaire and asked different questions from respondents related to the security issues of Public Cloud Computing and Private Cloud Computing in giant organizations. Security issues Analysis was done in Private and Public Cloud Computing in giant organizations and concluded the results on the basis of security of the data and reliability of the data. According to our findings we analyzed that main security issues in Private cloud computing are attacks from unknown and known threats, attacks hidden inside encrypted traffic, botnet and malware infections and unauthorized and unknown locations access to network and in Public Cloud computing main security issues are service or account hijacking, data scavenging, data leakage, denial of service, malicious VM creation and VM migration. The result according to our finding was that the Private Cloud Computing is safer than Public Cloud Computing in giant organizations.

5. FUTURE WORK

In future this work might be extended and restricted to Private Cloud Computing security threats. The future work might investigate more problems about security threats related to Private Cloud Computing. Future work, may also find solutions and recommendations to avoid security threats and attacks for Private Cloud Computing. Recommendations, investigation and solutions might be researched using surveys or modern Cloud Computing Literature.

6. ACKNOWLEDGMENTS

We are really thankful to Dr. Ramzan Talib, Dr. Kashif Hanif, Mr. Muhammad Umer Sarwar Department of Computer Science Govt College University Faisalabad and Akmal Rehan Department of Computer Science University of Agriculture Faisalabad who supported us and encourage to do some novel work for this paper. We are also thankful to Mr. Habib Ullah who helped us in deciding the topic, methods and analysis of this study. Their contribution is much helpful for us. We completed this work with full devotion under the kind supervision.

7. REFERENCES

[1] Nelson Gonzalez, Charles Miers, Fernando Red´ıgolo, Marcos Simpl´ıcio, Tereza Carvalho,Mats N¨aslund and Makan PourzandiPg, "A quantitative analysis of current security concerns and solutions for cloud computing", Journal of Cloud Computing: Advances, Systems and Applications, Springer,vol 1,issues 11,Pg no 1-18 2012.

[2] Greg Goth, "Mobile Security Issues Come to the Forefront", 1089-7801, IEEE, published by the IEEE computer society, pg 7-9, 2012.

[3] Keiko Hashizume, David G Rosado, Eduardo Fernández-Medina and Eduardo B Fernandez, "An analysis of security issues for cloud computing",Springer, Journal of Internet Services and Applications,vol 4,issues 5, Page 1-13, 2013.

[4] Kuyoro S. O., Ibikunle F. & Awodele O, "Cloud Computing Security Issues and Challenges",International Journal of Computer Networks (IJCN), Volume 3,Issue 5 , pg 247-255,2011.

[5] Elisa bertino, fellow, and ravi sandhu, "database security—concepts,approaches, and challenges" IEEE transactions on dependable and secure computing, vol. 2, no. 1, 1545-5971,pg 2-19,2005.

[6] Bernd Grobauer, Tobias Walloschek, and Elmar Stöcker "Understanding Cloud Computing Vulnerabilities", copublished by the ieee computer and reliability societies, 1540-7993, pg 50-57, 2011.

[7] Kevin Hamlen, Murat Kantarcioglu, Latifur Khan, "Security Issues for Cloud Computing", 10.4018/jisp. 2010040103, International Journal of Information Security and Privacy,vol 4,issues 2,page no. 39-51, April-June 2010.EARCH

[8] John Harauz, Lori M. Kaufman, bruce Potter, "Data Security in the World of Cloud Computing", IEEE ,1540-7993,copublished by the IEEE computer & reliability societies, Pg No 61-64, 2009.

[9] R Lakshman naik & s. S. V. N. Sarma,"A framework for mobile cloud computing", international journal of computer networking, Wireless and mobile communications (ijcnwmc), Issn 2270-1768,Vol. 3, issue 1,Pg No. 1-12,2013.

[10] K.Sravani, K.L.A.Nivedita," Effective Service Security Schemes In Cloud Computing",International Journal Of Computational Engineering Research ijcer Vol. 3,Issue 3,Issn 2250-3005, March 2013.

[11] https://en.wikipedia.org/wiki/Cloud_computing

[12] Amandeep, K. S. 2013. Analysis of Load Balancing Techniques in Cloud Computing. International Journal of Computers&Technology,4(3):124-143.