Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 6, June 2015, pg.230 – 234

RESEARCH ARTICLE

Study of Security Issues in Cloud Computing

Varsha

Student, M.Tech, CSE, Amity University, Haryana

Dembla.varsha@gmail.com

Amit Wadhwa

Assistant Professor, Dept.of Computer Science, Amity University, Haryana

awadhwa@ggn.amity.edu

Swati Gupta

Assistant Professor, Dept.of Computer Science, Amity University, Haryana

swattiguptta@gmail.com

ABSTRACT: As we all know Cloud computing is an emerging domain and security of the data must be protected over the network. There are some security issues occurring while using services over the cloud. In this paper, we investigate and carry out a small study and highlight all the issues of emerging over a cloud related to security of Cloud.

The major stress of our study based on existing literature, is to understand the concept of multi-tenancy security issue.

Keywords: Cloud Computing, Security issues and multi-tenancy.

1. INTRODUCTION

Cloud Computing provides shared resources and services via Internet. In last few years, usage of internet is increasing very rapidly which increases cost of hardware and software. So, the new technique known as cloud computing used to solve these problems by giving service when user demand over the internet and definitely it decreases the cost of hardware and software Services offered in cloud computing have various features like high scalability, reliability, flexibility and dynamic property.

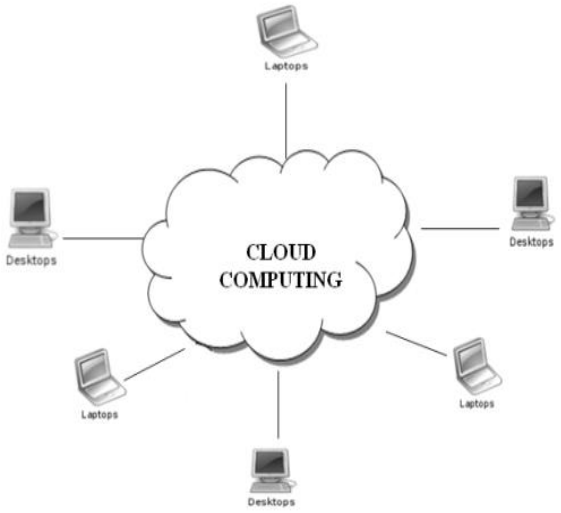

Fig1. Cloud computing [5]

1.1 Services Models

Three types of cloud services and user can use any services which are mentioned below:

- Software as Service (SaS)
- Platform as service (PaS)
- Infrastructure as service (IaS)

Software as Service (SaS): It is also called a delivery model where the software and the data which is associated with is hosted over the cloud environment by third party and that third party is called cloud service provider, like your Gmail account, you use that application on someone else's system.

Platform as Service (PaS): In this, you can use Web-based tools to develop applications so they run on systems software which is provided by another company, like Google App Engine.

Infrastructure as Service (IaS): It provides services to the companies with computing resources including servers, networking, storage, and data centre space on a pay-per-use basis.

1.2. Deployment models

There are three Deployment Models and are described below:

- Public Model
- Private Model
- Hybrid Model

Public Model: This infrastructure is available to the general public. As the name suggests, public cloud is a model in which resources are generally available to everyone or anywhere.

Private Model: This model is developed for the private organizations like one house and an organization and they can use it for their own purpose. This kind of a service is not accessed by everyone.

Hybrid Model: Hybrid Clouds are combination of public and private cloud in a same network. This can be done if private cloud need some important services from the public cloud like Private cloud can store some information on their private cloud and we can use that information on public cloud.

In cloud computing, there are many issues but security is the major issue which we will discuss further.

2. PROBLEM STATEMENT

Our research focus on the security issues of data over a cloud. We will broadly cover the aspect of multi-tenancy in cloud computing which will meet the challenges of security of data, so that the data will remain protected while being on the network.

3. LITERATURE REVIEW

Arijit Ukil, Debasish Jana and Ajanta De Sarkar [2]: In this paper, the problem of security in cloud computing has been analyzed. This paper gives security architecture and necessary support techniques for making our cloud computing infrastructure secured.

Rabi Prasad Padhy, Manas Ranjan Patra and Suresh Chandra Satapathy [3]: All the Security issues of cloud computing are highlighted in this paper, because of the complexity which users found in the cloud, it will be difficult to achieve end-to-end security. New security techniques need to be developed and older security techniques needed to be changed or improved.

Kashif Munir and Prof Dr. Sellapan Palaniappan [4]: In this study, we reviewed the literature for security challenges in cloud computing and proposed a security model and framework to make cloud computing environment secure.

Ayesha Malik and Muhammad Mohsin Nazir [5]: In this paper, various techniques have been discussed which helps to protect the data, secure data such as:

Mirage Image Management System [6]: This system addresses the problems related to safe management of the virtual machine images that summarize each application of the cloud [5].

Client Based Privacy Manager [7]: This technique helps to reduce the loss of private data and threat of data leakage that processed in the cloud, as well as provides additional privacy related benefits [5].

Transparent Cloud Protection System (TCPS) [8]: This provides protection system for clouds designed at clearly monitoring the reliability of cloud components. TCPS is planned to protect the integrity of distributed computing by allowing the cloud to monitor infrastructure components [5].

Secure and Efficient Access to Outsourced Data [9]: This Provides secure and efficient access to Outsourced data is an important factor of cloud computing and forms the foundation for information Management and other Operations [5].

Krešimir Popović, Željko Hocenski [10]: In this paper, security in cloud computing was discussed in a manner that covers security issues and challenges, security principles and security management models.

Takeshi Takahashi, Gregory Blanc*y*, Youki Kadobayashi*y*, Doudou Fall*y*, Hiroaki Hazeyama*y*, and Shin'ichiro Matsuo [11]: This paper introduced technical layers and categories, with which it recognized and structured security challenges and approaches of multitenant cloud computing.

Nagarjuna, C.C kalyan srinivas, S.Sajida,lokesh.[12]:In this paper the main issue with multi tenancy is that the clients use the same computer hardware to share and process information and the result is that tenants may share hardware on which their virtual machines or server runs, or they may share database tables.

4. SECURITY ISSUES IN CLOUD COMPUTING

Based on the study, we found that there are many issues in cloud computing but security is the major issue which is associated with cloud computing.

Top seven security issues in cloud computing environment as discovered by "Cloud Security Alliance" CSA are [1]:

- Misuse and reprehensible Use of Cloud Computing.
- Insecure API.
- Wicked Insiders.
- Shared Technology issues/multi-tenancy nature.
- Data Crash.
- Account, Service & Traffic Hijacking.
- Unidentified Risk report.

Misuse and reprehensible Use of Cloud Computing : Hackers, spammers and other criminals take advantage of the suitable registration, simple procedures and comparatively unspecified access to cloud services to launch various attacks like key cracking or password [4].

Insecure Application Programming Interfaces (API): Customers handle and interact with cloud services through interfaces or API's. Providers must ensure that security is integrated into their service models, while users must be aware of security risks [4].

Wicked Insiders: Malicious insiders create a larger threat in cloud computing environment, since consumers do not have a clear sight of provider policies and procedures. Malicious insiders can gain unauthorized access into organization and their assets [4].

Shared Technology issues/multi-tenancy nature: This is based on shared infrastructure, which is not designed to accommodate a multi-tenant architecture [4].

Data Crash: Comprised data may include; deleted or altered data without making a backup; unlinking a record from a larger environment; loss of an encoding key; and illegal access of sensitive data [4].

Account, Service & Traffic hijacking: Account or service hijacking is usually carried out with stolen credentials. Such attacks include phishing, fraud and exploitation of software vulnerabilities. Attackers can access critical areas of cloud computing services like confidentiality, integrity and availability of services [4].

Unidentified Risk Report: Cloud services means that organizations are less involved with software and hardware, so organizations should not be aware with these issues such as internal security, security compliance, auditing and logging may be overlooked [4].

We will discuss Multi-tenancy issue which we found a major concern in cloud computing.

5. SECURITY ISSUE: MULTI-TENANCY

Multi-tenancy is a major concern in cloud computing. Multi-tenancy occurs when various consumers using the same cloud to share the information and data or runs on a single server.

Multi-Tenancy in Cloud Computing occurs when multiple consumers share the same application, running on the same operating system, on the same hardware, with the same data-storage system and both the attacker and the sufferer are sharing the common server.

Architecture:

This architecture fully separates your information from other customer's information, while allowing us to roll out rapidly the latest functionality to each, all at once. This approach offers the most configurability and allows you to extract deep insight from your information

Oracle delivers a latest Multitenant architecture that allows a multitenant container database to grasp numerous pluggable databases. An existing database can simply be adopted with no application changes necessary.

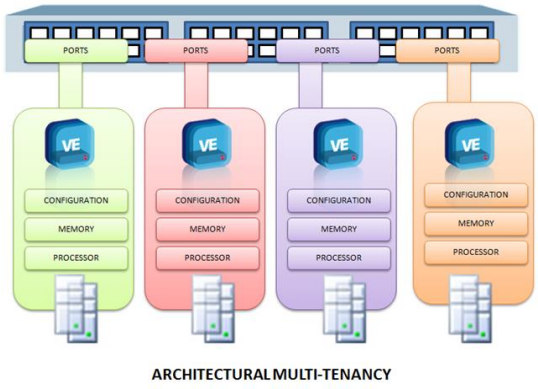

Fig2.Multi-tenancy architecture [13]

What Is Multi-Tenancy Able To Do?

Simplify Data Mining: Instead of being composed from various sources, all the information for consumers is stored in a single database scheme.

Decreases expenditure: Multi-tenancy reduces the overhead by amortizing it over many users, like they can charge for the certified software because everyone can run it on a single system, so only single certify will need to purchase

More elasticity: It provides the flexibility to import and export your information

6. FUTURE WORK

In future work, we could design a framework which could satisfy the security issues related to multi-tenancy.

7. CONCLUSION

Cloud computing is an immense prospect both for the businesses and the attackers – both parties be able to have their own reward from cloud computing. An infinite possibilities of cloud computing cannot be unseen only for the security issues reason – the unending analysis and research for robust, regular and integrated security models for cloud computing might be the only path of inspiration. Based on this fact that the impact of security issues in cloud computing can be decrease by multi-tenancy architecture.

REFERENCES

[1] "Security Guidance for Critical Areas of Focus in Cloud computing", April 2009, presented by Cloud Security Alliance (CSA).

[2] Arijit Ukil, Debasish Jana and Ajanta De Sarkar" A SECURITY FRAMEWORK IN CLOUD COMPUTING INFRASTRUCTURE "International Journal of Network Security & Its Applications (IJNSA), Vol.5, No.5, September 2013 DOI: 10.5121/ijnsa.2013.5502 11.

[3] Rabi Prasad Padhy, Manas Ranjan Patra and Suresh Chandra Satapathy ," Cloud Computing: Security Issues and Research Challenges", IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS) Vol. 1, No. 2, December 2011.

[4] Kashif Munir and Prof Dr. Sellapan Palaniappan," FRAMEWORK FOR SECURE CLOUD COMPUTING ", International Journal on Cloud Computing: Services and Architecture (IJCCSA), Vol.3, No.2, April 2013.
[5] Ayesha Malik, Muhammad Mohsin Nazir "Security Framework for Cloud Computing Environment: A Review", Journal of Emerging Trends in Computing and Information Sciences ©2009-2012 CIS Journal. All rights reserved, VOL. 3, NO. 3, March 2012 ISSN 2079-8407
[6] Jinpeng Wei, Xiaolan Zhang, Glenn Ammons, VasanthBala and PengNing, "Managing security of virtual machine images in a cloud environment", November 2009, Proceedings of the 2009 ACM workshop on Cloud computing security pages 91-96.
[7] Miranda Mow bray and Siani Pearson, "A Client- Based Privacy Manager for Cloud computing", June 2009, Proceedings of the Fourth International ICST Conference on communication system software and Middleware.
[8] Flavio Lombardi and Roberto Di Pietro, "Transparent Security for Cloud", March 2010, Proceedings of the 2010 ACM Symposium on Applied Computing, pages 414-415. Objectives of this paper is to study the major security issues arising in cloud environment.
[9] WeichaoWang, Zhiwei Li, Rodney Owens and Bharat Bhargava, "Secure and Efficient Access to Outsourced Data", ember 2009, Proceedings of the ACM workshop on Cloud computing security, pages 55-65.
[10] Krešimir Popović, Željko Hocenski,"Cloud computing security issues and challenges", MIPRO 2010, May 24-28, 2010, Opatija, Croatia.
[11] Takeshi Takahashi, Gregory Blancy, Youki Kadobayashiy, Doudou Fally, Hiroaki Hazeyamay, Shin'ichiro Matsuo,"Enabling Secure Multitenancy in Cloud Computing: Challenges and Approaches".
[12] Nagarjuna,C.C kalyan srinivas,S.Sajida,Lokesh" SECURITY TECHNIQUES FOR MULTITENANCY APPLICATIONS IN CLOUD", C.C. Kalyan Srinivas *et al*, International Journal of Computer Science and Mobile Computing Vol.2 Issue. 8, August- 2013, pg. 248-251.
[13]http://devcentral.f5.com/weblogs/images/devcentral_f5_com/weblogs/macvittie/WindowsLiveWriter/ArchitecturalMultitenancy_46C0/image1.png.

