ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

A Review on Security Issues in Cloud Computing

K Sri Vani

B.E Student, Dept. of ECE., M.N.M Jain Engineering College, Thoraippakam, Chennai, India

ABSTRACT: Cloud computing has evolved to be the basis for tomorrow's computing. The global computing infrastructure is rapidly heading towards cloud based architecture. Though it is important to take advantages of cloud based computing by means of deploying it in diversified sectors, the security aspects in a cloud based computing environment is of higher interest. Cloud services and its service providers are being evolved which has resulted in a new business trend based on cloud technology. This paper presents a review on the concepts and security issues of cloud computing.

KEYWORDS: Cloud computing; cloud network; cloud security; data encryption

I. INTRODUCTION

Cloud computing is an internet-based computing that provides shared computer resources, data and other required devices. In other words, cloud computing means storing and accessing data and programs over the Internet instead of your computer's hard drive. It supports shared pool of configurable computing resources with minimal management effort. Cloud computing offers sharing of resources in order to achieve coherent and economic scale over any other network. It offers service-oriented architecture and promotes "everything as a service". Also, cloud-computing providers offer their services with different models of which the three standard models per NIST are Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Cloud Computing Services provide information technology as a service over the Internet or dedicated network, with delivery on demand, and payment based on usage. Cloud computing services range from full applications and development platforms, to servers, storage, and virtual desktops. Cloud computing services work differently, depending on the provider. Many provide a browser-based dashboard that makes it easier for IT professionals and developers to order resources and manage their accounts. Infrastructure as a Service (IaaS) is a model of cloud computing that presents a virtualized resources for computing over the Internet. Platform as a service (PaaS) or application platform as a service is a form of cloud computing services that offers a platform allowing customers to develop, run, and manage various applications without the complexity of building and maintaining the infrastructure .Software as a service (SaaS) is a software distribution model in which a third-party provider hosts applications and makes them available to customers over the Internet. Cloud computing while reduces cost and heavy capital expenditure, it raises enormous security issues. In general,there are three different ways to deploy cloud computing resources: public cloud, private cloud and hybrid cloud. These security issues originate from various sources and creates a problem to the organization. This increases the complexity of computing platform and burdens the various aspects of the software. Thus, these security issues must be recognized accurately and rectified accordingly.

II. BASIC MODEL OF CLOUD COMPUTING

There are several security concerns associated with cloud computing. They fall into two broad categories: security issues faced by cloud providers and security issues faced by their customers. The provider must guarantee that their infrastructure is secured with protection for clients data and applications while using secure passwords and authentication measures.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

III. CLOUD COMPUTING SECURITY ISSUES

Data security involves encrypting the data and ensuring that appropriate policies are enforced for data sharing. The given below are the various security concerns in a cloud computing environment.

- Access to Servers & Applications
- Data Transmission
- Virtual Machine Security
- Network Security
- Data Security
- Data Privacy
- Data Integrity
- Data Location
- Data Segregation

A. *Data Transmission:*

Encryption mechanisms are used for data in transmission. It provides protection for data where the customer wants delivery of data by using authentication and integrity and is not modified during transmission. Several protocols are used for this purpose. In Cloud computing environment most of the data is not encrypted in the processing time. On the other end to process the transmitted data, for any application the data sent must be unencrypted. When an invader places him in the communication path between the users, there is a possibility that they can interrupt and change communications. According to the paper "Security in Data Storage and Transmission in Cloud Computing" written by Pradnyesh Bhisikar and Prof. Amit Sahu[1] high speed is the key issue in networking. They have provided a solution in securing the data without affecting the network layers and protecting the data from any kind of unauthorized entries into the server, keeping the data secured in server based on users choice of security system so that data is given high secure priority. A distributed scheme with two prominent features, opposing to its predecessors: Cloud storage enables users to remotely store their data and provides the freedom on-demand high quality cloud applications without the burden of local hardware and software management.

B. *Data Security:*

For general user, it is relatively easy to find the possible storage on the side that offers the service of cloud computing. To achieve the service of cloud computing, the commonly used communication protocol is Hypertext Transfer Protocol .The service provider must introduce additional security checks to ensure data security and prevent violations due to security vulnerabilities in the application or through malicious employees. This facilitates the use of strong encryption techniques for data security and fine-grained authorization to control access to data.According to the paper "Data Security Challenges and Its Solutions in Cloud Computing" written by R.Velumadhava Rao and K.Selvamani[2],presents security as a major concern since the data is transmitted to the remote server over a channel. They have declared that it is important for any organisation to address the security challenges before implementing Cloud Computing in their organization.The paper, "Data security in cloud computing" written by Ahmed Albugmi ,Madini.O.Alassafi and Robert Walters[3] , provides an insight on data security aspects for Data-in-Transit and Data-at-Rest. Their study was based on all the levels of SaaS (Software as a Service), PaaS (Platform as a Service) and IaaS (Infrastructure as a Service).The paper, "Research on data security issues of cloud computing",written by Chaoqun Yu,Lin Yang and Yuan Liu[4],states the art of the techniques on cloud computing data security issues, such as data encryption, access control, integrity authentication and other issues, which provides the basis to some important technical issues of the cloud computing data security.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

C. *Virtual Machine Security:*

Virtualization is one of the main element of a cloud. Virtual machines are dynamic in the sense that it can quickly be reverted to previous instances, paused and restarted, relatively easily. Ensuring that different instances running on the same physical machine are independent of each other is a major task of virtualization. The dynamic nature and potential for VM makes it complex to achieve and maintain consistent security. Vulnerabilities or configuration errors may be unnoticed and avails its propagation. Also, it is difficult to maintain an auditable record of the security state of a virtual machine at any given point in time. The other issue is the control of administrator on both host and guest operating systems.According to the paper, "Virtualization security for cloud computing service",written by Shengmei Luo,Zhaoji Lin and Xiaohua Chen[5], addresses the requirements and solutions for the security of virtualization in cloud computing environment. Also, a Virtualization Security framework was presented which contains two parts: virtual system security and virtualization security management. According to the paper, "Virtualization in Cloud Computing: NoHype vs HyperWall new approach", written by Meryeme Alouane and Hanan El Bakkali[6] , analyzes different approaches which solves the security issues of hypervisors, and also contributes to increase problem solving of security of hypervisors based architectures.

D. *Data Privacy:*

The data privacy is also one of the main concerns for Cloud computing. A privacy committee should also be created to make decisions related to data privacy. The requirement for this committee is to ensure that the organization is prepared to meet the data privacy demands of its customers and regulators. Data in the cloud is usually globally distributed which raises concerns about jurisdiction, data exposure and privacy. According to the paper, "Data Security and Privacy in Cloud Computing" written by Yunchuan Sun, Junsheng Zhang, Yongping Xiong, Guangyu Zhu[7] , emphasize on the fact that the data security and privacy protection issues are relevant to both hardware and software in the cloud architecture. It presents different security techniques and challenges from both software and hardware aspects for protecting data in the cloud and aimed at enhancing the data security and privacy protection for the trustworthy cloud environment. According to the paper, "Security and Privacy in Cloud Computing: Vision, Trends, and Challenges" written by,Zahir Tari, Xun Yi and Uthpala S.Premarathne[8], offers cost-effective solutions via a variety of flexible services. It concludes with a discussion on future research directions that might lead to more trustworthy cloud security and privacy.

E. *Data Location:*

Commonly, cloud users are not known with the exact location of the datacenter and also they do not have any control over the physical access to that data. Most of the cloud service providers have data centers . In most of the cases, this can be a major issue. Due to compliance and data privacy laws in various countries, locality of data is of utmost importance in many enterprise architecture. According to the paper, "Data Location and Security Issues in Cloud Computing", written by Zaigham Mahmood [9], cloud computing offers numerous benefits for the enterprises, though, there are also many issues, as with any new technology. One of the main issues relate to the security and confidentiality of customer data in terms of its location, relocation, availability and security. Some useful background information for organizations preparing to migrate to the cloud to take advantage of the latest computing paradigm.

IV. CONCLUSION AND FUTURE WORK

It can be noted that the security issues in cloud computing is a critical problem for the privacy of the organizations that are on cloud. There are significant and increasing amount of work on its analysis, however, only limited work has so far been. From all the paper references, it can be concluded that the identification of the security is of major concern and then provide optimum solutions to it without affecting the data.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

REFERENCES

1. Pradnyesh Bhisikar and Prof. Amit Sahu, "Security in Data Storage and Transmission in Cloud Computing",International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3, Issue 3, March 2013.
2. R. Velumadhava Rao and K. Selvamani, "Data Security Challenges and Its Solutions in Cloud Computing",International Conference on Intelligent Computing, Communication & Convergence, Procedia Computer Science 48 ,204 – 209,2015.
3. Ahmed Albugmi ,Madini.O.Alassafi and Robert Walters, "Research on data security issues of cloud computing",Future Generation Communication Technologies (FGCT),2016 Fifth International Conference,17-19 Aug 2016.
4. Chaoqun Yu,Lin Yang and Yuan Liu, "Research on data security issues of cloud computing",Cyberspace Technologies,International Conference ,8-10 Nov 2014.
5. Shengmei Luo and Zhaoji Lin and Xiaohua Chen, "Virtualization security for cloud computing service",International Conference on cloud and service computing;pp:174-179,2011.
6. Meryeme Alouane and Hanan El Bakkali, "Virtualization in Cloud Computing: NoHype vs HyperWall new approach",International Conference on Electrical and Information Technologies,pp:49-54,2016.
7. Yunchuan Sun, Junsheng Zhang, Yongping Xiong and Guangyu Zhu, "Data Security and Privacy in Cloud Computing", International Journal of Distributed Sensor Networks,Jan 2014.
8. Zahir Tari, Xun Yi and Uthpala S.Premarathne, "Security and Privacy in Cloud Computing: Vision, Trends, and Challenges", IEEE on cloud computing,Vol.2 Issue 2,pp:30-38.
9. Zaigham Mahmood, "Data Location and Security Issues in Cloud Computing", International Conference on Emerging Intelligence Data and Web Technologies, pp:49-54,2011.