A SURVEY ON DATA SECURITY IN CLOUD COMPUTING

N.Karunya[1], Dr.T.Deepa[2]

[1]Research Scholar in Computer Science, Sri Ramakrishna College of Arts and Science for Women, (India)

[2]Assistant professor in Computer Science, Sri Ramakrishna College of Arts and Science for Women, (India)

ABSTRACT

A Cloud computing is a distribution of on-demand services such as network, data storage, interchange the software and hardware to the business person as well as the particular user. Now a day's data storage is playing a major role in the computer technology for storing the large data. So the users are moving to the cloud for getting the low-cost and easy to get access to the data anywhere in the world at any time because the cloud is working on the internet connection. As in the cloud computing the data's are not stored in our own PC instead it is been stored in cloud server. So there are some security issues such as data integrity, data confidentiality and etc., to the cloud users. One of the major problems is securing the data's from the hackers to crack the information out of the users to store in the cloud. So in this paper, we will discuss the data security issue related work done with the help of several research papers. The aim of this paper is to give an easy understanding of the cloud computing and about the risk factor in the cloud during the data storage.

Keywords: Cloud Computing, Data Security and Data Security Techniques.

I. INTRODUCTION

Cloud computing is a type of Internet-based computing, it means to share the computer resources rather than having the servers or personal computers to handing the applications as well as the hardware devices. In cloud computing, the data's are not stored in any desktop or in PCs. The data can be stored in a remote location so it is easy to access the data from anywhere of the world at any time by using the internet topology. Some of the cloud computing advantages are: a) Lower-Cost Computers for Users, b) Lower IT Infrastructure Cost, c) Instant Software Updates, d) Improved Document Format Compatibility and etc. Yet cloud computing has some disadvantage and threats. One of the major problems is security and privacy concern. As in the cloud computing, the information is not stored in user's PCs, so it increases risk. Some of the cloud computing risk factors are: a) Requires a Constant Internet Connection, b) Doesn't Work Well with Low-Speed Internet Connection and c) Stored Data Might Not Be Secure.

II. CLOUD SERVICE MODEL

Cloud Services provides the two types of the model, A) Development model, and B) Deployment model.

A) DEVELOPMENT MODEL

In the development model is dividing into three different models,

a) SaaS (Software as a Service)

b) PaaS (Platform as a Service)

c) IaaS (Infrastructure as a Service)

a) SaaS (Software as a Service): SaaS is most probably the common type of the cloud services. In this model, a single application is delivered to the many knows of users from the vendor’s servers. The users don’t pay for the software but pay for the using it and access the applications via the API over the internet. So each organization move to the vendor server and this type of vendor is called tenant. This type of arrangement is called multi-tenant architecture. For example Caspio, Google Apps, Salesforce, Nivio, Learn.com.

b) PaaS (Platform as a Service): PaaS model computing the platforms such as sever, operating system, storage background of the computer is provided by a software engineer. For example Windows azure, Google App.

c) IaaS (Infrastructure as a Service): IaaS is a highly scaled redundant and shared computing infrastructure accessible using internet technology. Consists of servers, storage, security, databases, and other peripherals. For example Amazon EC2, S3, etc.

B) DEPLOYMENT MODEL

In the deployment model is dividing into three different models

a) Private Cloud

b) Public Cloud

c) Hybrid Cloud

d) Community Cloud

a) Private Cloud

The cloud is operated and managed by a single organization. It gives more security, reliability, performance and service.

b) Public Cloud

The cloud infrastructure is s set of computing resources provided by third- Party. The most popular public clouds are Amazon web services, Google App Engine, etc.

c) Hybrid Cloud

Hybrid Cloud is combination of any two different clouds to providing the computing resources.

d) Community Cloud

The cloud infrastructure is shared by several organizations. It is been managed by the organizations or a third party.

The examples of different cloud service models and their usage

	SaaS	PaaS	IaaS
Private	-	Apprenda, Stackato	VMware, Hyper-V, OpenStack, CloudStack
Community	-	NYSE Capital Markets Community Platform	NYSE Capital Markets Community
Public	Salesforce.com, QuickBooks Online, Office 635	Google App Engine, Microsoft Azure, VMware, CloudFoundry.com	Amazon EC2, Rackspace
Hybrid	-	Custom CloudFoundry.com	Custom, Rackspace

Table 1: cloud service models and their usage

III. DATA SECURITY TECHNIQUE IN CLOUD COMPUTING

Currently, cloud computing is adopting the many no of company because commercial profits by cloud but hackers or number of attackers are trying to crack the important data on the industrial information of the company. So the main concern about the company is securing the data onto the hackers. There are many studies that show the problems of the data stored in the cloud. Here we will discuss some problems of data security.

Encryption Algorithm

The security plays a very important role in cloud computing. Most of the cloud security is using the cryptographic algorithms. It is a form of coded data or non-readable format of the information for securing the data from the hackers. In these cryptographic techniques, a single level encryption algorithm used for securing the data but unauthorized person try to crack the data easily. It uses symmetric and asymmetric algorithm is used for encrypt and decrypt message.

Figure 1: Type of encryption

In symmetric (DES) algorithm private key (Session key) is used for encrypt the message and the same key is used for decrypt the message but the main problem is to maintain the key.

In asymmetric (RSA) algorithm there is two different types of key for encryption and decryption. The private key is used for encrypt the message and public key is used for decrypt the message.

In paper [1] the author's discuss the cryptography algorithms for data security in cloud. But the existing problems are single level cryptography algorithms, so unauthorized person can easily crack the data. Finally author summarized multilevel encryption and decryption algorithms, only the authorized person can access the data.

Proxy Re-Encryption Scheme

In this technique, the sever will encrypt the plain text into cipher text with the help of public key PKA and then this cipher text again encrypted with the help of another public key PKA by Proxy Re-Encryption key RKA->B and this way plain text will convert into cipher text. The information is encrypted before storing into the server. If the user wants to share the information, then it must be send a re-encryption key to the server. The server receives encryption message from the user then re-encrypt with the help of re-encryption key to the respective user. Thus, their system has confidentiality and secures the data.

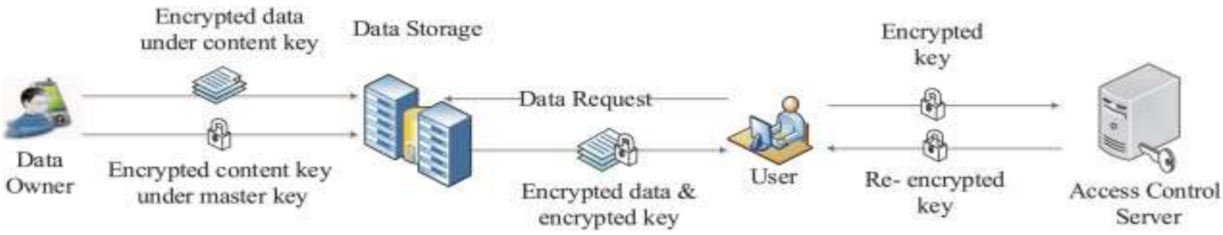

Figure 2: Proxy Re-Encryption Scheme

In paper [7] the authors discuss the proxy re- encryption schemes for data security in cloud. The summarization of the author's said introduction of the cloud computing, cloud storage system, cloud architecture and encryption techniques such as proxy re-encryption scheme and its types. For example Type Based Proxy Re-Encryption Scheme, Key Private Proxy Re-Encryption Scheme, etc.,

Playfair Cipher

Playfair cipher techniques using square matrix of 5x5 alphabetical letters arrangement. In this technique the matrix key is placed by the user by selecting the key. The balancing letters are arranged one by the one form place of key in the matrix. Different pairs are created by breaking plain text pairs. If the pairs having the same alphabet then it will be separated by letter "X". In the same way the pairs having the different alphabets in the same row each letter will change with letter a head of it. The next one is in the column of the pairs are interchanged with the letter below it.

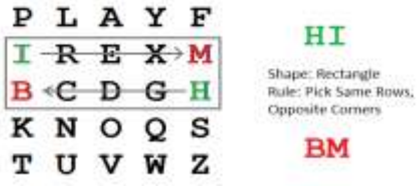

Figure 3: Playfair Cipher

The above figure explains the playfair cipher technique easily, the plain text “HI” is been encrypted as “BM” by using the same rows opposite corners rule.

Rail fence technique

Rail fence technique is the transposition ciphers. In this technique the plain text is written in the form of sequential diagonal. In the way of cipher text, the sequential diagonal is read as row by row.

For example,

“What is your name”

Now the message is encrypted in the form of

“waayunm

htroeasi”

So it cannot be understand by unauthorized user.

IV. CONCLUSION

The company’s are using cloud computing because it is cost efficient. The cloud computing has different security issues because the data’s are not stored in PC’s instead it is been stored in the cloud server but there are some security issues in cloud computing such as data integrity, data confidentiality and etc., to the cloud users. So in this research we discussed definition of the cloud, introduction of the cloud, security issues and their techniques.

REFERENCES

[1]. Sajjan R.S, Vijay Ghorpade and Vishvajit Dalimbkar ,“A Survey Paper on Data security in Cloud Computing”, International Journal of Computer Sciences and Engineering,Volume-4, Special Issue-4, June 2016.

[2]. Noman Mazher, Imran Ashraf ,“A Survey on data security models in cloud computing”, Noman Mazher et al Int. Journal of Engineering Research and Applications, Volume-3, Issue 6, Nov-Dec 2013.

[3]. Jasleen Kaur, Ms.Anupma Sehrawat, Ms.Neha Bishnoi,“Survey Paper on Basics of Cloud Computing and Data Security”, International Journal of Computer Science Trends and Technology (IJCST) – Volume 2, Issue 3, May-Jun 2014.

[4]. S. Muthakshi M.Sc., M.Phil., Dr. T.Meyyappan M.Sc., MBA. M.Phil., Ph.d., ”A Survey on Security Services In Cloud Computing”, International Journal of Engineering Trends and Technology (IJETT) - Volume4 Issue7- July 2013.

[5]. Harshitha. K. Raj, “A Survey on Cloud Computing”International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 7, July 2014.

[6]. Y. Ghebghoub, S. Oukid, and O. Boussaid, ”A Survey on Security Issues and the Existing Solutions in Cloud Computing”, International Journal of Computer and Electrical Engineering, Vol. 5, No. 6, December 2013.

[7]. Rutuja Warhade, Prof. Basha Vankudothu, “A Survey on Proxy Re-encryption Schemes for Data Security in Cloud”, International Journal of Advance Research in Computer Science and Management Studies, Volume 2, Issue 12, December 2014.