Review on Cloud Computing Security Issues and Encryption Techniques

Jaspreet Singh[1], Sugandha Sharma[2]
[1]Research Scholar, Deptt. of CSE, Chandigarh University, Punjab (India)
[2]Assistant Professor, Chandigarh University, Punjab (India)

_____

Abstract - **Cloud computing is the latest technology in the modern world. Cloud computing is the present technology in the field of distributed computing. The adoption of this technology is growing day by day because it facilitates the users to utilize the services through making use of shared pool of resources without the installation of any software. It provides various services to the user at lower cost and easily. But security is the critical inhibitor that are faced by cloud computing and it makes the use of cloud computing more difficult. To solve these problems, we have some encryption algorithms which provide security to the data stored on cloud. In this paper, an effort is made to review the security problems and the encryption algorithms that provide security to the cloud data.**

Keywords - **Cloud computing, Service Models, Security issues, Encryption Algorithms**
_____

I. INTRODUCTION

Cloud computing is a growing technology which has gained significant attention recently from the industry field and academia. It offers services through the internet. User can deploy the services of different software by using cloud computing without buying or installing them on their own computers. It is the logical representation of the internet in the diagrams that's why is called cloud computing [2]. According to the definition of NIST, cloud computing can be defined as computing paradigm for enabling on-demand, useful network access to the large pool of configurable computing amenities. Cloud computing is the extension-internet based technology of the distributed computing, which uses the internet and the remote servers to support applications and data. According to the Gartner [3] cloud computing can be defined as a method of computing that delivered IT capabilities 'as a service' to the users by using internet. Some of the foreign companies that are leading in the cloud computing are Google, Yahoo, Amazon and IBM.

A cloud is a huge pool of easily and accessible virtualized resources, such as development services, hardware and software. These pools of resources are composing a type utilized by pay-per-use model. In the cloud, user uses any device which has the capability of using a network that connects it to a server at any other location. In the cloud computing, there is no need to end user to store data on their device because user can store their data on cloud or any remote server.

In cloud computing, three service models and the four deployment models are used. The service models are that which provide services to the customers on pay-per-use basis, environment for developers to build the applications and storage space to store their data. The deployment models that make the software available for use to the customers or the organizations. In the service-oriented architecture, the software as service, platform as a service and infrastructure as a service can be combined to provide the functionality of large application. Cloud computing reduces the cost of hardware that is used by end user's.

II. SECURITY ISSUES

In cloud computing, security is considered to be a crucial barrier in its path to success. Many researchers have discussed the new research issues that are raised by cloud computing. The personal data security is the crucial concern in the cloud computing environment. That's why in cloud computing or because of some other many reasons cloud computing needs to increase the security of data stored on cloud. Most of the security issues in the cloud computing are:

Location Transparency
It is the one of the well-known work ability for cloud computing, which is a security problem at the same time, without knowing the exact location of the data storage.

Distributed Denial of Service
It can be a potential or serious problem for cloud computing. In cloud computing infrastructure, it is the major common attack until now and there is no option to mitigate this type of problem.

Data Protection
Multiple users's shared the cloud computing infrastructure at any point of time. The user's data is under provider's control that is stored and processed in the shared environment. Any malicious inside the cloud can interfere with the user data that may cause some security problems because of the lack of transparency about the data storage etc. makes the requirement of data protection in the cloud environment more important.

Multi-Tenancy
A single cloud provider serves multiple cloud users by sharing of resources it causes some security issues like virtualization and resource management for isolation.

Network Security
It is difficult to track the network traffic and performance due to the creation of invisible networks by virtual servers.

Data Access
This issue is mainly related to the security policies that are given to the customers or users while accessing cloud data. In typical situation, an organization can use the cloud that is provided by other provider to conducting its business processes. Each employee of a organization have considered policies to access the business data stored on cloud. To avoid, disruption by the unauthorized access the security policies must be closely followed by cloud.

Data confidentiality issue
In cloud computing, users can store their data and information on remote servers owned by others or accessed through the internet. The data confidentiality issues are raised when a government agency or any other entity shares the information stored on cloud.

Data Breaches
In cloud environment, various users' data and the organizations data is lie together. The cloud environment breaching will potentially attack the data of all users.

III. ENCRYPTION TECHNIQUES

To improve the cloud computing security various encryption algorithms and techniques are used that helps the cloud user to store their data on cloud with minimum risk. In this paper, we made a review on various algorithms that are used for encrypt the data.
Amit et al. [1] described a Bi-Directional DNA encryption algorithm for enhancing the security in cloud computing. However, there are no existing algorithm which also focuses on non-English user of the cloud computing not only on ASCII character set. But this technique can be used with Unicode characters to enhance the security of cloud computing [1]. This paper described the various steps of conversion from one form to another to encrypt the data with higher complexity that are described in figure 1.

```
┌──────────────────────┐
│  Unicode plain text  │
└──────────────────────┘
           ↓
┌──────────────────────┐
│   Convert into ASCII  │
└──────────────────────┘
           ↓
┌──────────────────────┐
│ Hexadecimal converter │
└──────────────────────┘
           ↓
┌──────────────────────┐
│   Binary Converter    │
└──────────────────────┘
           ↓
┌──────────────────────┐
│  DNA Digital Coding   │
└──────────────────────┘
           ↓
┌──────────────────────┐
│   PCR Amplification   │
└──────────────────────┘
           ↓
┌──────────────────────┐
│   Amplified Message   │
└──────────────────────┘
           ↓
┌──────────────────────┐
│   Encrypted Message   │
└──────────────────────┘
```
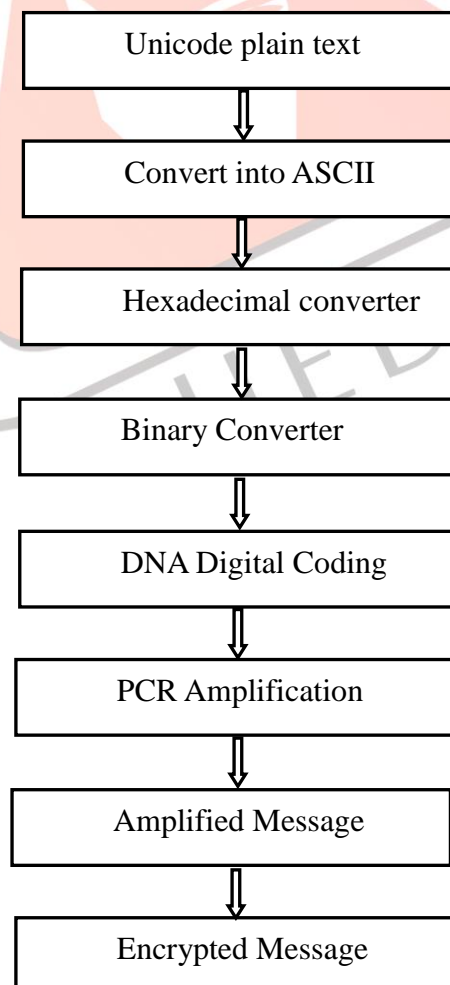
Figure: 1

Various algorithms such as RSA, AES, DES, Blowfish etc are used in this paper for making cloud data secure described by

Rachna et al. [3]. These various algorithms have been used in this paper to deal with the various security issues and secure the data from hackers or unauthorized person. This paper has made the comparison of these algorithms to make sure that which algorithm is best to provide security for cloud data [3].

P Subhasri et al. [4] proposed a multilevel encryption algorithm which will be more secure than the other encryption techniques. In this, writer described two types of encryption method to make the clod data more secure. The first method is the Rail fence cipher algorithm that will use for Transposition and the other one is the Caeser cipher for substitution. In this method it is difficult to understand the cipher text compared with the other techniques. The writer is using a combination of three different algorithms to improve the security in the paper [6].

Dimpi Rani et al. [6] depicted that the combination of RSA and Blowfish will be more secure, when it will be used with the digital signature. The writer explained the various vulnerabilities and the threats that affect can cloud computing and cloud environment [9]. The study defined in this paper elaborate the various issues of security that are seriously affect the cloud infrastructure [8].

IV. CONCLUSION

Cloud computing is relatively a new technology that provides vast benefits to the users. Cloud computing has huge visions, but the security hazards placed in cloud computing approach are directly related to the benefits that it offers. For both the businesses and the hackers or attackers, cloud computing is a great chance and profitable. Security is a inflexible requirement for cloud computing environment. We have presented the various cloud computing security issues and the solutions for this.

In this review, we also represents the various encryption techniques to make the data secure on cloud. There are various encryption algorithms are explained in this paper that are RSA, AES, DES and the Blowfish etc.

V. REFERENCES

[1] Amit et al. [1] "Enhancing Security in Cloud Computing Using Bi-Directional DNA Encryption Algorithm" Springer 2015

[2] Aized et al. [2] "Encryption Techniques For Cloud Data Confidentiality", International Journal of Grid Distribution Computing Vol.7, No.4 (2014)

[3] Rachna et al. [3] "Secure User Data in Cloud Computing Using Encryption Algorithms", International Journal of Engineering Research and Applications (IJERA) , Vol. 3, Issue 4

[4] Dr.A.Padmapriya et al. [4] "Cloud Computing: Security Challenges & Encryption Practices", Volume 3, Issue 3, March 2013

[5] Dimpi et al [5] "Enhance data security of private cloud using encryption scheme with RBAC", International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 6, June 2014

[6] Aman et al. [6] "Comparative Analysis between DES and RSA Algorithm's", IJARCSSE, Volume 2, Issue 7, July 2012

[7] P.Subhasri et al. [7] "Multilevel Encryption for Ensuring Public Cloud", IJARCSSE, Volume 3, Issue 7, July 2013

[8] Monjur et al. [8] "Cloud Computing and Security Issues in the Cloud", International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.1, January 2014

[9] Keiko et al. [9] "An analysis of security issues for cloud computing", Journal of Internet Services and Applications 2013

[10] Iiango et al. [10] "Research Agenda in Cloud Technologies"