www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 4 Issue 2 February 2015, Page No. 10430-10433

Survey On Business Model For Cloud Computing Using Rsa & Aes Algorithm

Prachi Bhagat[1], Asmita Dhamale[2], Ishita Saraf[3], Madhuri Thorat[4]

Savitribai Phule Pune University,BSCOER
Pune, India
isaraf39@gmail.com[3]

Abstract: ***Storing of confidential data has become a most important thing these days. It is necessary that the data stored must remain secured and should be accessed at the client's request. Cloud computing helps us to store our files on the cloud. Hence it is very efficient and helpful for a client's point of view. But there are some security issues in this type of data storage. Thus by using encryption and decryption techniques we can encrypt and decrypt the files as per the need of the client.***

Keywords: Cloud Computing, encryption, decryption, data security.

1. INTRODUCTION

Cloud Computing has become a most hot topic in past 2-3 years. Before cloud computing was introduced the data used to be stored on data storage servers. It was sometimes impossible to store a high amount of data on the servers. And in case of server crash the complete data would get lost. Security was the most difficult issue in these type of storage servers. Firewalls were the only option for these kind of storages. Hence adding a firewall to the network was the only solution for security issues. But just adding a firewall was not enough, it is rather important to hide the confidential data from the intruders. The intruders are nothing but the third parties that are trying to interfere in between the communication. For any client server application security is the most important aspect. Hence it has become necessary to provide security in such client server applications.

Now-a-days, as distributed system and network computing are used on large scale, security is becoming one of the risk factor an important issue in the future. User confidential data is not secured and safe in this fast developing of distributed computing technologies. As there are much more changes of getting data hacked by any unauthorized user.

Generally, in the text-based password, the password is easy to guessing the others user. The one user is easily find out the password of second user and easily login her\his account. So, there is the need to finding the more secure password and to generate the graphical password. This would rather improve the quality of the project and make the software application more reliable and safe for any client server application in a distributed network or any desktop application as well.

Cloud computing collects all the computing resources and software required to work on them. Cloud computing provides an efficient technique to provide an accurate information and proper service to users and enterprises. In this process, user does not have to take care of how to buy servers, resources and software. Depending upon the user need, the user can buy the computing resource through Internet.

a) Software as a Service (SaaS) is an On demand model and offers an application, such as ERP, CRM, Google Apps etc. on demand over the internet.

b) Platform as a Service (PaaS) provider sells a complete development platform including the necessary built-in services, such as MySQL database, LDAP, Net Beans software, on demand over the network.

c) Infrastructure as a Service (IaaS) is an foundation layer for other two delivery models and offers hardware and software infrastructure components, such as compute, storage, systems etc. Currently three deployment models have been identified for cloud architecture by the National Institute of Standards and Technology.

1.1. Private Cloud

In private cloud, cloud providers and cloud consumers are part of the same company and the IT department of a company acts as the cloud provider and offers a cloud service that can be used by internal units to deploy and run business applications via private networks (in-house or hosted)..

1.2. Public Cloud

A public cloud can use anyone who has access to an internet connection, is able to pay, and is aware of the specific cloud services can use it on demand. Practically everyone on the Web can take advantage of public cloud services.

1.3. Hybrid Cloud

Hybrid clouds represent a combination of both private and public cloud models. For example, a Company implements a private cloud to support business-critical services and utilizes the public cloud in an on-demand fashion for non-critical services. Therefore, this type of cloud model might be of interest to large, global enterprises. It also provides much better data security for the company itself as it is connected via a combination of public and private networks.

2. LITERATURE SURVEY

2.1 Business Model for Cloud Computing Based on a Separate Encryption and Decryption Service.

This study proposes a business model for cloud computing based on the concept of separating the encryption and decryption service from the storage service. Furthermore, the party responsible for the data storage system must not store data in plaintext, and the party responsible for data encryption and decryption must delete all data upon the computation on encryption or decryption is complete.

In this method cloud service provider has responsible for data storage and data encryption/decryption tasks, which takes more computational overhead for process of data in cloud server. The main disadvantage of this method is, there is no control of data for data owner i. e, data owner has completely trusted with cloud service provider and he has more computational overhead[1].

2.2 Blowfish Algorithm

This paper proposed a model to encrypt the data in one service provider and store the data in the different service provider. So once the data is stored in the application it gets encrypted

and the encrypted data will not be present in the encryption service provider. Thus the storage of the data will be in the encrypted format and the administrators and the staffs have no knowledge about the encrypted keys and the service providers of the encryption and decryption[3].

2.3 Encryption and Decryption service

One service provider operates the encryption and decryption system while other providers operate the storage and application systems**.** the HRM Service System transmits the user ID to the Storage Service System where it searches for the user's data. This data is encrypted so, once found, a request must be sent to the Encryption/Decryption Service System along with the user ID. The Storage Service System executes the transmission of encrypted client data and the user ID to the Encryption/Decryption Service System. There is communication between the Encryption/Decryption server and the storage server due to which the data can be hacked easily, this is the major drawback of this paper [4].

2.4 Separate Encryption/Decryption Services for Cloud Computing

This paper aims to introduce the problems and challenges concerned with the presently used cloud computing services, which is based on a merged encryption/decryption services with storage devices & for solution to this problem we are designing a business model. If a cloud system is responsible for both tasks on storage and encryption/decryption of data, the Storage system administrators may simultaneously obtain encrypted data and decryption keys. This allows them to access information without authorization and thus poses a risk to information privacy. In such cases there need to separate the encryption/decryption services from storage devices to divide the authority of storage management dept which blocks the Storage system administrators for disclosure of users data[6].

The proposed paper uses AES algorithm which is of 128 bit and uses symmetric keys. The use of symmetric key causes encryption and decryption keys to be same which reduces its security level. Anyone who gets access to the encryption key can eventually decrypt the data.

2.5 Data Security Using Key Rotation.

We propose an efficient data encryption to encrypt sensitive data before sending to the cloud server. This exploits the block level data encryption using 256 bit symmetric key with rotation. In addition, data users can reconstruct the requested data from cloud server using shared secret key. We analyze the privacy protection of outsourced data using experiment is carried out on the repository of text files with variable size. The security and performance analysis shows that the proposed method is highly efficient than existing methods performance [2].

The disadvantage in this paper is that it uses a 256 bit symmetric key for encryption and decryption, which decreases the security level because after receiving all the requested blocks from the cloud server, user decrypts all the encrypted blocks using same secret key before accessing it.

2.6 The Comprehensive Approach for Data Security in Cloud Computing

This paper, will gives a descriptive knowledge regarding cloud computing privacy and security issue provided by encryption and decryption services. If a cloud system is performing a task of storage of data and encryption and decryption of data on the same cloud then there are much more chances of getting access to the confidential data without authorization. This increases the risk factor in terms of security and privacy [5].

This paper helps us on proposes a business model for cloud computing which focused on separating the encryption and decryption service, from the storage service provided by service provider.

3. BUSINES MODEL FOR CLOUD COMPUTING USING RSA AND AES, FOR DATA SECURITY

3.1. Core Concept

The concept is based on separating the storage and encryption/decryption of user data as shown in fig.1. When the authorized user request a file from the encryption/decryption server, cloud service provider gets the encrypted file blocks from the encryption/decryption server and sends to the user. After receiving all the requested blocks from the cloud server, user decrypt all the encrypted blocks using different secrete key before accessing it.The client will send the file for storage to the database server, where the user id and the encrypted data are stored together.

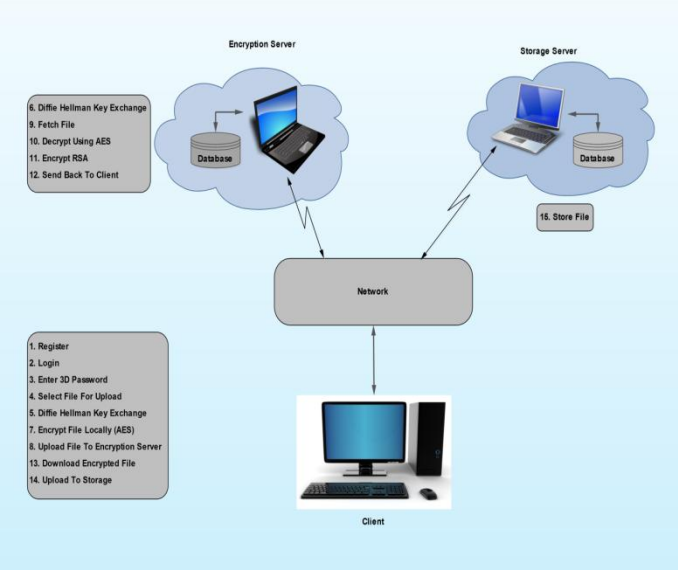

Figure 1: Encryption/Decryption as an independent service.

At the time of file retrieval the client will request to the storage server and then the encrypted data will be sent to the client by the storage server. Finally the encryption/decryption server will encrypt/decrypt the file and send it to the client. This study emphasis that encryption/decryption cloud services must be provided independently by a separate provider.

4. CONCLUSION

This paper presents various security issues in cloud environment and also present that we can get better security by separating encryption/decryption service from storage service. Reduce computational overhead for process of data in cloud server and reduce the burden of data owner.

References

[1] "A Business Model for Cloud Computing Based on an Encryption and Decryption Service" Jing-Jang Hwang and Hung-Kai Chuang Department of Information Management. Hang Gung University Kwei-Shan Tao-Yuan, Taiwan Yi-Chang Hsu and Chien-Hsing Wu Graduate Institute of Business and Management Chang (2011 IEEE)

[2]"Data Encryption and Decryption Algorithms using Key Rotations for Data Security in Cloud System. "Prakash G L1 ,Dr. Manish Prateek2 and Dr. Inder Singh3.1Research Scholar, Department of Computer Science and Engineering, UPES, Dehradun, Email:glprakash78@gmail.com 2Associate Dean, Centre for Informat ion Technology, UPES, Dehradun 3Assistant Professor, Centre for Informat ion Technology, UPES, Dehradun.

[3] "Cloud Computing a CRM Service based on separate Encryption and Decryption using Blowfish Algorithm" Rajiv R Bhandari M-Tech Student, Department of IT NRI Institute of Information Science and Technology Bhopal, (MP) India. rajivbhandari@ymail.com Prof.Nitin Mishra Professor, Department of IT NRI Institute of Information Science and Technology Bhopal, (MP) India. nitin.nriist@gmail.com

[4]" Efficient Encryption and Decryption Services for Cloud Computing." Vishakha Lokhande #1, Prasanna Kumari P.*PG Student, Lords Institute of Engg & Tech, JNTU, Hyderabad, AP, India*Associate Professor, Department of CSE, Lords Institute of Engg & Tech,JNTU, Hyderabad, AP, India.*

[5]"The Comprehensive Approach for Data Security in Cloud Computing": A Survey,Nilesh N. Kumbhar ,Virendrasingh V.Chaudhari ,Mohit A.Badhe.

[6] "Business Model based on a Separate Encryption & Decryption Services for Cloud Computing." International Journal of Advances In Computer Science and Cloud Computing, ISSN: 2321-4058 Volume- 1, Issue- 2, Nov-2013.Business Model Based On A Separate Encryption & Decryption Services For Cloud Computing 12. 1A. R. KAMBLE, 2SANKET TARAL, 3PRASAD KUBADE, 4ABHISHEK WAGH, 5NIKHIL SHETE.

[7]"A Secure Cloud Computing Model Based on Multi Cloud Service Providers." International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper Available online at: www.ijarcsse.com. Mooga Masthan Dora Babu Sudarsa M.Tech 2nd year, Dept. of CSE, ASCET, GUDUR, India
Associate Professor, Dept. of CSE, ASCET, GUDUR, India