BUSINESS MODEL FOR CLOUD COMPUTING USING RSA & AES ALGORITHM

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

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.**

***Index Terms*— Cloud Computing, encryption, decryption, data security.**

I. 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.

A. 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)..

B. 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.

Manuscript received April, 2015.
Prachi Bhagat, *Computer Engineering, BSCOER, Pune,India,8551882727*
Asmita Dhamale, *Computer Engineering, BSCOER, Pune,India,9665725105*
Ishita Saraf, *Computer Engineering, BSCOER, Pune,India, 8446133036*
Madhuri Thorat, *Computer Engineering, BSCOER, Pune,India,8408899553*

ISSN: 2278 – 1323

C. 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.

II. LITERATURE SURVEY

A. 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.

B. 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].

III. LIMITATIONS OF PREVIOUS SYSTEM

The main disadvantage of the previous system 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.

IV. PROBLEM STATEMENT

To develop a system for secure data storage which can be deployed on cloud. By using AES and RSA together more security can be provided to the confidential data.

V. PROPOSED SYSTEM

A. User Authentication

This module describes the user authentication for the Service System.The user has to login to the service System, after the user logs into the system, if the Service System requires any client information, it will execute a Data Retrieval Program. When this data needs to be saved, it will execute a Data Storage Program. When a user wants to access the Cloud Service, he must first execute the Login Program which uses a One-Time 3D Password.

B. User Data Request

After the user's login has been successfully verified, if the Service System requires client information from the user, it sends a request for information to the Storage Service System. In this step, the 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. The above-mentioned Data Retrieval Program requires the collaboration of three different cloud service systems. We have used different methods of system collaboration which are already supported by mature technologies, including two systems based on Universal Description Discovery and Integration (UDDI), Web Service Description Language (WSDL), and Simple Object Access Protocol (SOAP) to use Web Services or transmit Extensible Markup Language (XML) formatted data.

C. Data Storage Program:

This module also involves the collaboration of three cloud service systems: Service System, Encryption/Decryption Service System, and Storage Service System. The client sends a Data Storage Request to the Service System which then initiates the Data Storage Program, requesting file uploading/downloading service. Storage Service System where the user ID and files are stored together.

VI. PROPOSED ALGORITHMS

A. User Authentication

Step 1: The user inputs login credentials to the System.
Step 2: Apply symmetric key-based security

ISSN: 2278 – 1323

Step 3: Provide 3D Password.
Step 4: Check for client information request.
Step 5: Execute Data Retrieval Program.
Step 6: Check for data needs to be saved.
Step 7: Execute Data Storage Program.

B. User Data Request

Step 1: Check user's login successfully verified.
Step 2: Sends request for information to the Storage Service System.
Step 3:System transmits the user ID to the Storage System.
Step 4: Searches for the user's data.
Step 5: Send request to the Encryption/Decryption Service System
along with the user ID.

C. Data Storage Service

Step 1: Retrieve client Data Storage Request to the System.
Step 2: Initiates the Data Storage Program.
Step 3: Request data encryption from the Encryption/Decryption Service System.
Step 4: Establish a secure data transfer channel to transmit the user ID and data.
Step 5: Transfer the data to the Storage System.
Step 6: Delete all unencrypted and decrypted user data.

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

A. 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.

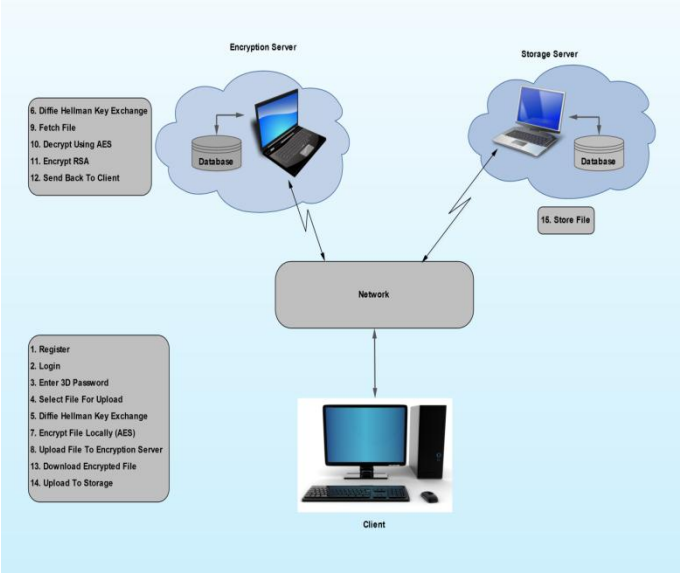

Figure 1: Encryption/Decryption as an independent service.

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.

VIII. EXPERIMENTATION

The following tables show the time required for uploading and downloading the files.
Table I states the time required for uploading only. Table II states the time required for downloading.

TABLE I
EXECUTION TIME FOR UPLOADING FILE OF 10 PEOPLE

User No	File Size	Time Required for file Upload (Full Process)	User No	File Size	Time Required for file Upload (Full Process)
1	1 KB	4 sec	6	17 KB	10 sec
2	5 KB	6 sec	7	14 KB	10 sec
3	16 KB	10 sec	8	4 KB	5 sec
4	9 KB	9 sec	9	3 KB	3 sec
5	7 KB	6 sec	10	8 KB	7 sec

ISSN: 2278 – 1323

TABLE II
EXECUTION TIME FOR DOWNLOADING FILE OF 10 PEOPLE

User No	File Size	Time Required for file Upload (Full Process)	User No	File Size	Time Required for file Upload (Full Process)
1	1 KB	3 sec	6	1 KB	11sec
2	5 KB	5 sec	7	14 KB	11 sec
3	16 KB	11 sec	8	4 KB	5 sec
4	9 KB	10 sec	9	3 KB	3 sec
5	7 KB	7 sec	10	8 KB	9 sec

IX. 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, Associate.

ISSN: 2278 – 1323

Prachi Mahesh Bhagat
BE,Computer Engineering at BSCOER,Pune.
Under the Savitribai Phule University Of Pune.

Asmita Kailas Dhamale
BE,Computer Engineering at BSCOER,Pune.
Under the Savitribai Phule University Of Pune.

Ishita Sunil Saraf
BE,Computer Engineering at BSCOER,Pune.
Under the Savitribai Phule University Of Pune.

Madhuri Bhagwanta Thorat
BE,Computer Engineering at BSCOER,Pune.
Under the Savitribai Phule University Of Pune.

