Data Security in Cloud Computing Using Separate Encryption/Decryption Cloud Service

Prajakta R Rajapure
Dept. of Computer Engineering
PES's Modern College of Engineering
Pune, India
prajaktar35@gmail.com

Deepali S Khandzode
Dept. of Computer Engineering
PES's Modern College of Engineering
Pune, India
deepali.khandzode@gmail.com

Swati N Ranpise
Dept. of Computer Engineering
PES's Modern College of Engineering
Pune, India
ranpise.swati@gmail.com

Meghana R Kanthale
Dept. of Computer Engineering
PES's Modern College of Engineering
Pune, India
meghana.kanthale@gmail.com

***Abstract*— Usually users store data on internal storage and protect that data by installing firewalls. In cloud computing, the data will be stored in storage provided by service providers. Service provider must have a visible way to protect their user's data, especially to prevent the data from unauthorized access by insiders. Encrypting data is one form of data protection mechanism. Usually in cloud computing, single cloud is responsible for storing and encrypting data. But in this case, cloud service providers internal staff can access the encryption and decryption keys and access user data. Thus, user's data is at stake. So we propose a system for data security in cloud computing based on separate encryption/decryption service from storage service. We propose a system in which storage is provided by storage cloud service and security is provided by Trusted Computing Platform(TCP) cloud service. Storage cloud service only stores user data already encrypted through TCP, but does not have access to decryption keys. As it does not have access to decryption keys it cannot decrypt data encrypted by TCP service.Storage service provider also cannot store decrypted data. TCP service involves encryption/decryption of user data. TCP cannot store decrypted or encrypted user data.TCP cannot access user data without decryption keys.In this way, we increase the security of data on cloud as even the administrators of the cloud could not access user data.

Keywords- *Cloud computing; encryption cloud service, decryption cloud service; Storage service provider; Trusted Computing Platform*

*****

I. Introduction

Cloud computing is one of the most widely used technology in today's world. Before the development of cloud computing, industries used to store their data internally on storage media, to which security was provided by including firewalls to prevent external access to the data. Cloud allows customer to have a regular access to their data, but customers are concerned with the security aspect of it. So the cloud storage service providers must have in place data security practices to ensure that their clients' data is safe from unauthorized access and disclosure.

A Common way in which security is provided to user data, is by encrypting the data before storage. Usually in cloud computing environment, a user's data can also be stored following additional encryption, but if the storage and encryption of given user's data is performed by the same service provider, the service provider's internal staff can use their decryption keys and internal access privileges to access user data. From the user's view this could put his stored data at risk of unauthorized disclosure.

In today's world, security is an important issue. Cloud allows customer to have a regular access to their data, but customers are concerned with the security aspect of it. For providing security, we propose a theory that instead of storing and securing data on storage cloud itself, we will distribute the task. We will encrypt the data using one cloud i.e. TCP cloud and store the encrypted data on separate cloud i.e. storage cloud. Also we will provide channel security for secure exchange of keys.

In addition, those working with the data storage system will have no access to decrypted user data, and those working with user data encryption and decryption will delete all encrypted and decrypted user data after transferring the encrypted data to the system of the data storage service provider.

As per the proposed system, the data storage cloud service provider is responsible to store the user's encrypted data, but does not have access to Decryption key. Thus, the storage system can only retrieve encrypted user data, but cannot decrypt it. The cloud computing system responsible for encrypting user data i.e. Trusted Computing Platform (TCP) has responsibility of overall encryption keys required for data encryption but, given that the TCP provider does not store the user's data, internal mismanagement of the decryption keys still poses no risk of unauthorized access to the user's data.

II. Literature Review

A. Origin and Definition of Cloud Computing

Cloud computing services use the Internet as a transmission medium and transform information technology resources into services for end-users, including software services, computing platform services, development platform services, and basic infrastructure leasing.

As a concept, Cloud is a concept in which large number of computers are connected together via internet as shown in fig 1.

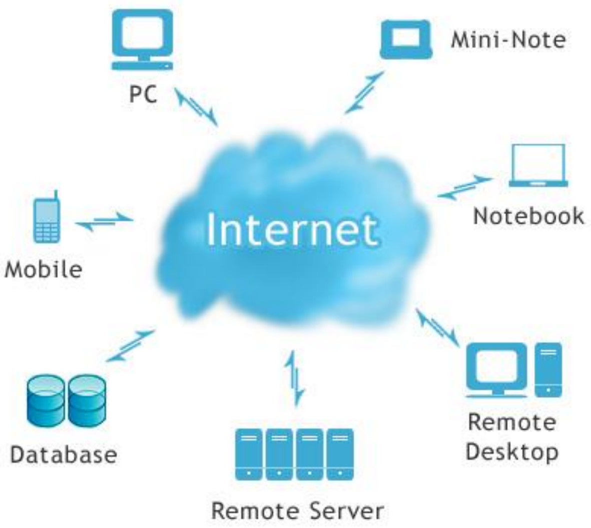

Figure 1. Cloud Computing concept.

Some scholars find cloud computing similar to grid computing [2]. The literature contains many explanations of cloud computing [3]. After examining scholarly definitions of cloud computing, Rodero-Merino, Vaquero , and Lindner Caceres, suggested that cloud computing could be defined as the integration of virtual resources according to user requirements, flexibly combining resources including hardware, development platforms and various applications to create services[4].

The special features of cloud computing include the storage of user data in the cloud and the lack of any need for software installation on the client side. As long as the user is able to connect to the Internet, all of the resources in the cloud can be used as client-side infrastructure. Generally speaking, cloud computing applications are demand-driven, providing services according to user requirements, and service providers charge by instances of use, or defined period.

B. Cloud Computing Business Models

The hardware and architecture required for providing cloud computing environment services is similar to most computer hardware and software systems. The hardware in modern personal computer (i.e. CPU,HDD, optical drive, etc.) performs basic functions such as performing calculations and storing data. The operating system (e.g. Windows XP) is the platform for the operations of the basic infrastructure, and text processing software such as MSWord and Excel are application services which run on the platform.

The architecture of cloud services can be divided into three levels: infrastructure, platform and application software [4]. Application software constructs the user interface and presents the application system's functions. Though the functions of the operations platform, the application can use the CPU and other hardware resources to execute calculations and access storage media and other equipment to store data.

Building a cloud computing application as a service requires infrastructure, platform and application software which can be obtained from a single provider or from different service providers. If the revenue for cloud services primarily comes from charging of infrastructure , this business model can be referred to as Infrastructure as a Service (IaaS). If revenue comes from charging for the platform, the business model can be referred to as Platform as a service (PaaS). If revenue primarily comes from charging for applications or an operating system, the business model can be referred to as Software as a Service (SaaS).

C. Methods For Protecting Data Stored in a Cloud Environment

Common methods for protecting data include encryption before storage, user authentication procedures before storage or retrieval, and developing secure channels for data transmission. These protection methods normally require cryptography algorithms and digital signature techniques, which are explained below:

Common data encryption methods consist of symmetric and asymmetric cryptography algorithms.

This form of encryption and decryption process uses
secret key. Asymmetric cryptography, on the other hand, uses two different keys, a “public key” for encryption, and a “private key” for decryption. Example include RSA [5] cryptography and Elliptic Curve Cryptography (ECC) [6].Generally speaking, symmetric cryptography is more efficient, and is suitable for encrypting large volumes of data. Asymmetric cryptography requires more computation time and is used for the decryption keys required for symmetric cryptography.

The use of passwords as an authentication process is more familiar to general users, but messages sent by the user are vulnerable to surreptitious recording by hackers who can then use the data in the message to log into the service as the user. In more advanced authentication systems, the system side will produce a random number to send the user a challenge message, asking the user to transmit an encrypted response message in reply to the challenge message, thus authenticating that the user will not be allowed access. In the process of challenge and response the client’s encrypted key uses the client’s password to convert a derived value and in this program, communication between the client and server is unique, and a hacker using an old messages would fail to access the system. In addition, the One Tim Password (OTP) authentication system differs from most peoples’ conception of password[7].Most people understand a password to be a password chosen by the user to be meaningful, and can be used again and again. The emphasis of OTP, however is the single-use nature of the password.

After receiving authentication from the user, the system side must create a secure transmission channel to exchange information with the user. The Secure Sockets Layer (SSL) is a common method of building secure channels [8], primarily using RSA encryption to transmit the secret keys needed for the both sides to encrypt and decrypt data transmitted between them. When using cryptographic technology to protect user data, the keys used for encryption and decryption of that data must be securely stored. In particular, cloud computing service providers must have specific methods for constraining internal system management personnel to prevent them from obtaining both encrypted data and their decryption keys-this is critical to protecting user data.

III. A Proposed System For Cloud Computing Based On Separate Encryption And Decryption Service

A. *Core Concepts*

This study proposes a system for Cloud Computing based on the concept of Separate Encryption and Decryption Cloud Service.

The concept is based on separating the storage and encryption/decryption of user data, as shown in Fig.2.In this system, Encryption/Decryption as a Service and Storage as a Service(SaaS) are not store unencrypted user data and, once the Encryption/Decryption Service provider has finished encrypting the user data and handed it off to an application, the encryption/decryption system must delete all encrypted and decrypted user data.

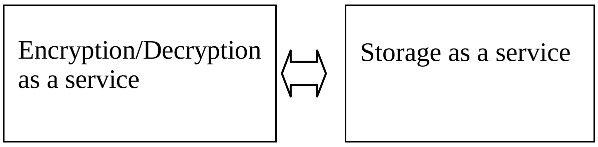

Figure 2. Encryption/Decryption as an independent service

B. System Architecture

To illustrate the concept of our proposed system, Fig. 3 presents system architecture for uploading file and Fig.4 presents systems architecture for downloading file

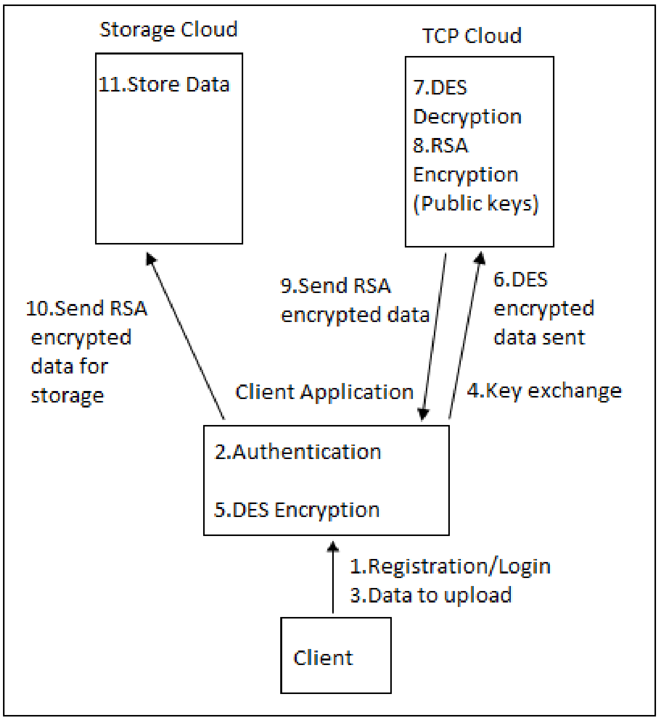

Figure 3. Uploading a File.

In order to access the system client must register to the system. After the client is successfully registered as a first step he must login to the system. Secondly, authentication will take place. In the third step, client will select the file which he has to upload on to the cloud. To establish a communication between the client application and TCP cloud, Diffie Hellman key exchange takes place at the fourth step. In step five, client application performs DES encryption of the data which is selected by the client. This DES encrypted data is then sent to the TCP cloud in step six. On receiving the encrypted data, TCP cloud performs DES decryption to decrypt that data in step seven. In step eight, TCP cloud again encrypts that data using RSA and this data is sent to the client application in step nine. In step ten, the client application will send this data to the storage cloud and it is securely stored at the storage cloud in step eleven. After sending RSA encrypted data to storage cloud, TCP cloud deletes this data from TCP cloud, so that encrypted data is on storage cloud and decryption keys are on the TCP cloud and hence data will be securely stored.

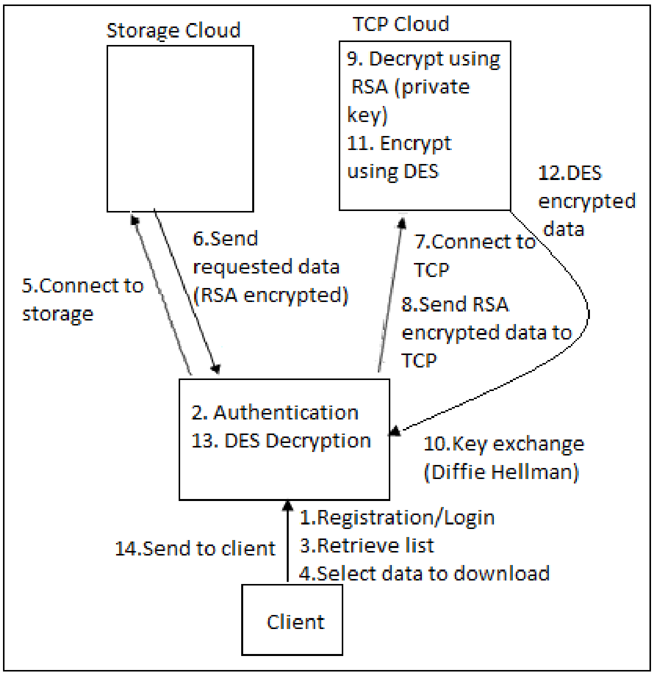

Figure 4. Downloading a File.

Once the client has successfully uploaded the data to cloud, he can download that data at any time provided network connection is available. Firstly he must login to the system. Secondly authentication will takes place. After successful authentication, he will receive the list of files which he has already uploaded in step three. In step four, he will select the file to be downloaded. In step five, client application connects to the storage cloud and asks for the file requested by the client. In step six, storage cloud fetches that file and finds that the file is encrypted using RSA and it does not have keys to decrypt it. So storage cloud connects with TCP cloud in step seven and sends RSA encrypted file to TCP cloud in step eight. In step nine, TCP cloud then decrypts the data as it has the decryption keys. As the data should reach the client securely, at step ten Diffie Hellman key exchange takes place. TCP cloud then encrypts the data using DES in step eleven and in step twelve, this encrypted data is sent to client application. In step thirteen, client application performs DES decryption and finally sends requested data to client in step fourteen.

In this way, data is uploaded and downloaded to cloud in secure manner.

IV. Benefit Analysis And Discussion

Cloud computing environments include three types of service: infrastructure, platform and software. To the user, cloud computing visualizes resources and, to access services, the user only requires a means of accessing the Internet, e.g., a smart phone, or even a smart card or other active smart chip, thus reducing purchasing and maintenance costs or software or hardware. Because ley industrial data is stored on the service provider's equipment, the service provider must protect the user's data, for example, by encrypting the user's data prior to storage. However, this leaves the service provider's high-privilege internal staff (e.g., system administrators) with access to both the Decryption key and the user's encrypted data, exposing the user's data to risk of potential disclosure.

For cloud computing to spread, users must have a high level of trust in the methods through which service providers protect their data. This study proposes a system for Decryption Service, emphasizing that authorization for storage and encryption/decryption of user data must be vested with two different service providers. The privileges of Storage as service provider include storing user data which has already been encrypted through Encryption/Decryption System, but does not allow this service provider to access Decryption key or allow for the storage of decrypted data. Also, the privileges of Encryption/Decryption service provider includes management of the key required for the encryption/decryption of user data, but not the storage of decrypted or encrypted user data. In this new system, User data in Storage Service System is all saved encrypted. Without the decryption key, there is no way for the service provider to access the user data. Within the Encryption/Decryption Service System there is no stored user data, thus removing the possibility that user data might be improperly disclosed. The core concept of this study is consistent with division of management authority to reduce operational risk, hence avoiding the risk of wrongful disclosure of user data.

V. References

[1] Jing-Jang Hwang, Hung-Kai Chuang, Yi-Chang Hsu and Chien-Hsing Wu , "A Business Model for Cloud Computing Based on a Separate Encryption and Decryption Service," International Conferences on Digital Object Identifier, pp. 1-7, 2011.

[2] M. Baker, R. Buyya, and D. Laforenza, "Grids and grid technologies for wide-area distributed computing," International Journal of Software: Practice and Experience, vol.32, pp. 1437-1466, 2002.

[3] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, "Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing as the 5th utility," Future Generation Computer Systems, vol. 25, issue 6, pp. 599-616, June 2008.

[4] L. M. Vaquero,L. Rodero-Merino,J. Caceres, and M. Lindner, "A break in the clouds: towards a cloud definition," ACM SIGCOMM Computer Communication Review, vol. 39, no. 1, pp. 50-55, January 2009.

[5] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public key cryptosystems", Communications of the ACM, vol. 21, no. 2, pp.120-126, 1978.

[6] [6] V. Miller, "Uses of elliptic curves in cryptography," Advances in Cryptology - CRYPTO '85, Lecture Notes in Computer Science, pp. 417-426, 1986.

[7] L. Lamport, "Password authentication with insecure communication," Communications of the ACM, vol. 24, no. 11, pp. 770-772, 1981.

[8] A. Elgohary, T. S. Sobh, and M. Zaki, "Design of an enhancement for SSL/TLS protocols," Computers & Security, vol. 25, no. 4, pp. 297- 306,June 2006.