Secure and efficient cloud computing data framework

Ms.M.Aruna,UG SCHOLAR (CSE),

Ms. K.Karthika,UG SCHOLAR (CSE),

Ms.p.Manimegalai,UG SCHOLAR (CSE),

Mr.M.Mailsamy M.E ., ASSISTANT PROFESSOR (CSE)

VIVEKANANDHA COLLEGE OF ENGINEERING FOR WOMEN ,

tiruchengode, tamilnadu, india.

mailsamym@gmail.com

m.manishaaruna@gmail.com

karthisweety1624@gmail.com

manimegalai1096@gmail.com

ABSTRACT

with the popularity of cloud computing, mobile devices can store/retrieve personal data from anywhere at any time. Consequently, the data security problem in mobile cloud becomes more and more severe and prevents further development of mobile cloud. There are substantial studies that have been conducted to improve the cloud security. However, most of them are not applicable for mobile cloud since mobile devices only have limited computing resources and power. Solutions with low computational overhead are in great need for mobile cloud applications. In this paper, we propose a lightweight data sharing scheme (ldss) for mobile cloud computing. It adopts cp-abe, an access control technology used in normal cloud environment, but changes the structure of access control tree to make it suitable for mobile cloud environments. Ldss moves a large portion of the computational intensive access control tree transformation in cp-abe from mobile devices to external proxy servers.

1. INTRODUCTION

cloud computing is a very useful solution to many individual users and organizations. It can provide many services based

on different needs and requirements. There are many issues related to the user data that need to be addressed when using cloud computing. Among the most important issues are: data ownership, data privacy, and storage. The users might be satisfied by the services provided by the cloud computing service providers, since they need not worry about the maintenance and storage. Furthermore, to reduce the user revocation cost, it introduces attribute description fields to implement lazy-revocation, which is a thorny issue in program based cp-abe systems. The experimental results show that ldss can effectively reduce the overhead on the mobile device side when users are sharing data in mobile cloud environments.

2. PROJECT OVERVIEW

There are two main ways to do encryption today. The first kind of encryption, called **symmetric cryptography shared secret encryption**, has been used since ancient egyptian times. This form of encryption uses a secret key, called the **shared secret**, to scramble the data into unintelligible gibberish. The person on the other end needs the shared secret (key) to unlock the data—the encryption algorithm.

Cloud computing presents a new way to supplement to current consumption and delivery model for IT services based on the internet. Lack of consumer in cloud service providers with compliance across geographic boundaries.

Emphasis is on data protection, but the notion of accountability encompasses more than just privacy.

3. BLOCK DIAGRAM

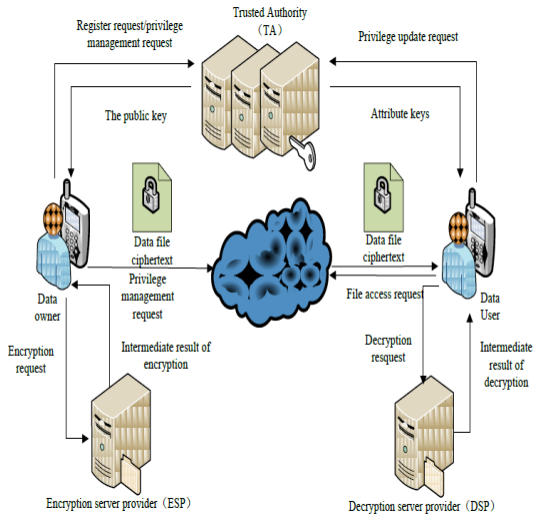

Figure 3.1 Secure and efficient cloud computing data framework

4. HARDWARE DESCRIPTION

4.1 DATA ENCRYPTION STANDARD (DES)

Des is the original standard that the u.s. Government began promoting for both government and business use.

Originally thought to be practically unbreakable in the 1970s, the increase in power and decrease in cost of computing has made its 56-bit key functionally obsolete for highly sensitive information. However, it is still used in many commercial products and is considered acceptable for lower security applications. It also is used in products that have slower processors, such as smart cards and appliance devices that can't process a larger key size.

4.2 TRIPLEDES

Tripledes, or 3des as it is sometimes written, is the newer, improved version of des, and its name implies what it does. It runs des three times on the data in three phases: encrypt, decrypt, and then encrypt again. It actually doesn't give a threefold increase in the strength of the cipher (because the first encryption key is used twice to encrypt the data and then a second key is used to encrypt the results of that process), but it still gives an effective key length of 168 bits, which is plenty strong for almost all uses.

4.3 AES

When the u.s. Government realized that des would eventually reach the end of its useful life, it began a search for a replacement. The national institute of standards and technology (nist), a government standards body, announced an open competition for a new algorithm that would become the new government standard. There were many competitors including rc6, blowfish by renowned cryptographer bruce schneier, and other worthy algorithms. They settled on aes, which is based on an algorithm called rijndael, designed by two belgian cryptographers. This is significant because they used an open competition to decide on the standard. Also, selecting an algorithm by two non-american developers with no significant commercial interests helped to legitimize this selection worldwide. Aes is rapidly becoming the new standard for encryption. It offers up to a 256-bit cipher key, which is more than enough power for the foreseeable future. Typically, aes is implemented in either 128- or 192-bit mode for performance considerations.

4.4 SECURE SOCKET LAYER (SSL)

This protocol was designed specifically for use on the web, although it can be used for almost any type of tcp communications. Netscape originally developed it for their browser to help stimulate e-commerce. Ssl provides data encryption, authentication on both ends, and

message integrity using certificates. Most of the time, ssl is used when connecting to a web server so that we know the information we send it is being protected along the way. Most people don't even realize that ssl is running in the background. Usually it only authenticates one end, the server side, since most end users don't have certificates.

5.MODULES AND DESCRIPTION:

Module in this project:

5.1 Data owner (do)

5.2 Data user (du)

5.3 Trust authority (ta)

5.4 Encryption service provider (esp)decryption service provider (dsp)

5.5 Cloud service provider (csp)

5.1 DATA OWNER (DO)

The data owner send data to the cloud. Since the cloud is not credible, data has to be encrypted before it is uploaded. The do defines access control policy in the form of access control tree which policies are such as read the data, write the data. Data files to assign which attributes a du should obtain if he wants to access a certain data file. In ldss, data files are all encrypted using symmetric encryption mechanism, and the symmetric key for data encryption is also encrypted using attribute based encryption (abe).

5.2 DATA USER (DU)

The data owner, tpa is present on equal level of authority. Data owner firstly should register or login on website then as it nothing but work like acsp (cloud service provider) then he can upload his own files on cloud in encrypted format. Data user can register or login on website for access for files ,after login of data user on cloud server then request goes to the data owner then data owner decide the approve of files access to user or not. Data user has acknowledgment from data owner if he approves the request of data user.

5.3 TRUST AUTHORITY (TA)

Third party authorization is used to monitories the data owners activities also it can check the integrity, durability of files which are uploaded by data owner on mobile cloud computing. Trusted authority (ta) also generates the report for data owner.

While requesting of data user of some kind of data from cloud, data owner select the role for data user and also after approval of users request he send the public key to data user through the email then data user can

retrieve the information from cloud by entering the key on website but this information it in the form of encryption so to decrypt that data .data owner provide the private key to data user from mail. Then by using this key data user can decrypt that data

5.4 ENCRYPTION SERVICE PROVIDER (ESP) & DECRYPTION SERVICE PROVIDER (DSP)

To relieve the overhead on the client side mobile devices, encryption service provider (esp) and decryption service provider (dsp) are used. Both the encryption service provider and the decryption service provider are also semi-trusted. We modify the traditional cp-abe algorithm and design an ldss-cp-abe algorithm to ensure the data privacy when outsourcing computational tasks to esp and dsp, also we used the aes (advanced encryption standard) algorithm to encrypt and decrypt the overall data which are uploaded on mobile cloud by data owner.

5.5 CLOUD SERVICE PROVIDER (CSP)

The csp is considered honest and curious. Second, all the sensitive data are encrypted before uploaded to the cloud. Third, user authorization on certain data is achieved through encryption/decryption key distribution. In general, we can divide these approaches into four categories: simple cipher text access control, hierarchical access control, access control based on fully homomorphic encryption and access control based on attributebased encryption (abe). Finally, we implement a data sharing prototype framework based on ldss and also used the aes(advance encryption standard) algorithm for purpose of encryption of data which are uploaded on mobile cloud computing

6. EXISTING SYSTEM

An encryption operation which takes one minute on a pc will take about half an hour to finish on a mobile device. Furthermore, current solutions don’t solve the user privilege change problem very well. Such an operation could result in very high revocation cost. This is not sapplicable for mobile devices as well. Clearly, there is no proper solution which can effectively solve the secure data sharing problem in mobile cloud. As the mobile cloud becomes more and more popular, providing an efficient secure data sharing mechanism in mobile cloud is in urgent need.

7. PROPOSED SYSTEM

In this paper, we propose a lightweight

data sharing scheme (ldss) for mobile cloud Computing environment. We design an algorithm called ldss-cp-abe based on attribute- based encryption (abe) method to offer efficient access control over cipher text. We use proxy servers for encryption and decryption operations. In our approach, computational intensive

Operations in abe are conducted on proxy servers, which greatly reduce the computational. Overhead on client side mobile devices. we processed using a basic level of security instead of using the same high level of security. Table I shows the performance of our framework.

CONCLUSION

Instead of offloading all codes directly to the remote cloud, we employ mobile devices nearby to form a local mobile cloud with low communication delay with the wearable devices. simulation show that algorithm quickly converge to performance close to optimal solution. we proposed an efficient confidentiality-based cloud storage framework that enhances the processing time and assures confidentiality and integrity through data classification

and applying TLS, AES and SHA based on the type of classified data. The efficiency of our proposed framework has been

shown through conducting simulations.

REFERENCE

[1] R. K. Ko, P. Jagadpramana, M. Mowbray, S. Pearson, M. Kirchberg, Q. Liang, and B. S. Lee, “Trustcloud: A framework for accountability and trust in cloud computing,” in Services (SERVICES), 2011 IEEE World Congress on. IEEE, 2011, pp. 584–588.

[2] v. Guzhov, k. Bazhenov, s. Ilinykh, and a. Vagizov, “cloud computing security issues,” in the 2-nd indo-russian joint workshop on computa

Tional intelligence and modern heuristics in automation and robotics,2011, pp. 128–133.

[3] f. Ogigˇau-neamt¸iu, “cloud computing security issues,” journal of Defense resources management (jodrm), no. 02, pp. 141–148, 2012.

[4] f. Ogigˇau-neamt¸iu, “cloud computing security issues,” journal of Defense resources management (jodrm), no. 02, pp. 141–148, 2012.

[5] t. Brindha, r. Shaji, and g. Rajesh, “a survey on the architectures Of data security in cloud storage infrastructure,” engineering and

Technology (ijet), vol. 5, pp. 1108–1114, 2013.

[6] y. Wei, z. Jianpeng, z. Junmao, z. Wei, and y. Xinlei, “design and Implementation of security cloud storage framework,” in instrumenta-Tion, measurement, computer, communication and control (imccc), 2012 second international conference on. Ieee, 2012, pp. 323–326.