The Reseach of AES algorithm and application in cloud storage system

Zhiyi Fang[1,a], Yao Sun[1,b], Yujing Sun[2,c],Jianming Yang[2,d]

[1]College of Computer Science and Technology Jilin University Changchun, 130012, P.R. China

[2]Beijing ACEWAY Communication Co.,Ltd

[a]fangzy@jlu.edu.cn, [b]syloyy@163.com, [c]sunyj@aceway.com.cn, [d]yangjm@aceway.com.cn

Keywords: AES algorithm; cloud storage

Abstract. With the rapid development of Internet technology, the data of the users' information have raised up largely, so internet storage became more and more important in today's life. In this paper, a cloud storage system has been designed and implemented. By using AES encryption algorithm, the security mechanism of users' files uploading and downloading has been researched

Introduction

With the intelligence and networking development of the electronic products, meeting the needs of the public users or the businesses for portable and high capacity has become the most important in development of the information industry. Cloud storage has become the preferred option to provide portable storage service for ordinary users, solve the requirement of large capacity, the difficulty of management and the requirement of high generic extensions. The security mechanism of cloud storage system is also becoming more and more important. So in this paper, the AES encryption algorithm has been researched and a cloud storage system has been designed and implemented base on the AES encryption algorithm.

Related work

Cloud storage arouses everybody's enthusiasm and ushered in the rapid market growth as soon as that enter China, that has emerged a large number of cloud storage application in just a few short years, such as Huawei, 360, kinsman has launched its own cloud storage applications. Some enterprises based on the existing user base, establishing and developing their own cloud storage applications, some enterprises halfway decent, with his bare hands to build his own cloud storage system, the reason is only one: they all look good which cloud storage market [1]. At same time ,the user are also showing an unprecedented support and enthusiasm in cloud storage.115network location announced their registered users has exceeded 30 million, while Huawei's network location also announced its own registered users has exceeded 20 million, which not only reflect the cloud storage application of high-speed development, comparing with the amount of Internet users, 420 million Internet users, this is to remind us, the cloud storage market of our country still has a considerable development space. However, large user base of cloud storage system performance and load problem poses a challenge [2].

Open business capacity platform is a server platform based on PaaS (Platform as a service) business model. Currently, many cloud storage services are realized through outsourcing, cloud storage service operators do not need to build their own file storage system, they can use the interfaces provided by platform to outsource the data store tasks. Some of these platforms are focus on cloud storage, some have much business and cloud storage is a part of them. What the well-known cloud storage Drop Box used is Amazon S3 platform. There are two operators in this kind of cloud service, the cloud service operator and the data storage operator. The cloud service operators communicate with the users and manage user's information while the latter try their best to manage the users' files on the platform. Users didn't feel the data storage operators but they stay with them all day long. With the development of mobile Internet, developing the open business capacity platform applies to mobile Internet is on the time. The platform can not only provides

cloud service but also provides telecommunications business capacity and other business capacities.

The system described by this article is based on the platform of opening business ability of China Unicom, provides network disk service. This is a test program of the platform provides business ability for the mobile Internet. The system can not only meets the needs of the project but also provides some common functionality, such as the upload or download of files, some file operation and the management of the information of users.

Research of AES algorithm

AES encryption algorithm is a kind of symmetric encryption algorithm[3]. It is published by the national institute of standards and technology (NIST) in October 2000. AES encryption algorithm is supported in PHP programming language. By Installing PHP Mcrypt extension modules which provide RIJNDAEL 256 - bit encryption algorithm, so that we can invoke the PHP functions to encryption and decryption users' files[4]. The structure of AES is seen in figure 1.

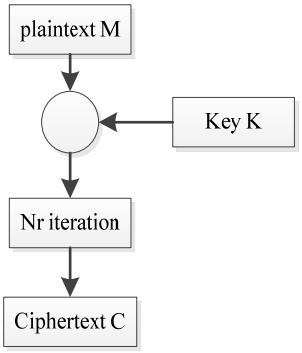

Fig. 1 AES structure

AES provides plaintext length should be 128bit, its key length has three optional values: the first value is 128bit, the second value is 192bit, and the third value is 256bit. According to the secret key length, AES algorithm completed Nr iterations. The relationship of Nr times and key length is in the table below.

Table1 relationship of Nr times and key length

Key length	128	192	256
Nr times	10	12	14

The 128-bit input plaintext is divided into 16 bytes, usually represented as a 4 * 4 matrix; each matrix element is 8 bits (one byte). The plaintext sequence from left to right is S00, S10, S20, S30, S01, S11, S21, S31, S02, S12, S22, S32, S03, S13, S23, S33. The plaintext block of any stage in the wheel transform is named "state"[5] .

The initial plaintexts block M:

$$\begin{matrix} S_{00} & S_{01} & S_{02} & S_{03} \\ S_{10} & S_{11} & S_{11} & S_{13} \\ S_{20} & S_{21} & S_{12} & S_{23} \\ S_{30} & S_{31} & S_{13} & S_{33} \end{matrix}$$

AES encryption has the following steps:

(1). Conducted a round of secret key plus operator first.

(2). Conducted Nr-1 iterations. Use S block to substitute each byte; do the displacement for the substitution result, then do the mix column transform operation. After these, a round of secret key plus operator is conducted.

(3). Final round transform include byte substitution, line transformation and key processing operation.

Encryption process is shown in figure 2:

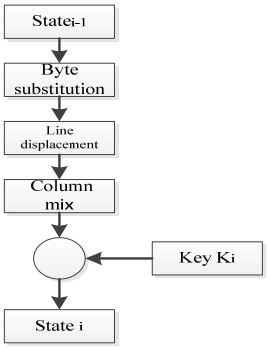

Fig. 2 Encryption process

The design of cloud storage system and application of AES algorithm

The system described by this paper was developed by LNMP (Linux + Nginx + MySQL + PHP) and CI (CodeIgniter) framework. The PC version of the system used some technologies such as Ajax, JQuery. The mobile terminal portion selected some necessary functions, using JQueryMobile to develop mobile terminal pages. The final purpose of this system is to make a test program of the open platform; the system is the Cloud Storage part of the project. In addition, we want to provide a reference for future the actual development of secure cloud storage services based on open-platform.

(a) System architecture design

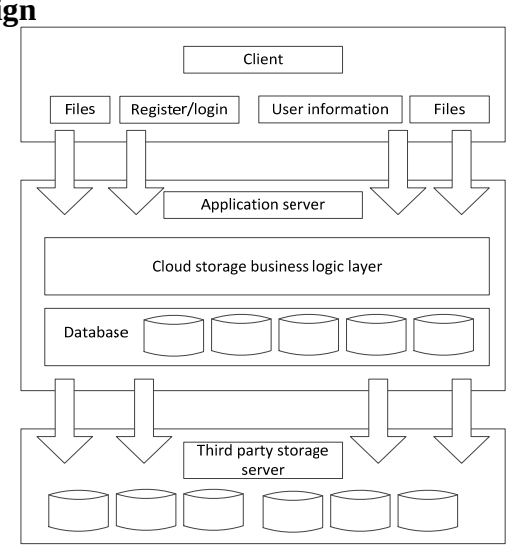

Fig. 3 Architecture of cloud system

The module of system file operation uploads, downloads and deletes data by call to the interface of open service platform for cloud storage, and the platform provides Restful Web Service interface. When you register at the platform, you will get AppKey and AppSecret then you will receive an authentication named token, finally, authorization is done. These systems make a simple encapsulation to the platform interface, and provide a test of PHP SDK. The cloud storage interface uploads files by means of PUT, and sends a ask for file-download to platform server by means of GET, then server return the link of file-download, and sends a ask for file-delete to the platform server by means of GET to delete files, finally server will return a corresponding result.

(b) Application of AES algorithm

File encryption and decryption was respectively used in the file upload and download modules.

Encryption process

(1). Bytes transformation: AES defines an S-box matrix composed with a 16 * 16 bytes array. Take the high 4 bit of 8 matrix elements as the row value and low 4 bit of 8 matrix elements as the column value searching S-box table, and the corresponding value obtained is the result of the transformation matrix elements.

(2). Row displacement: displace a row of the State matrix.

(3). Column mix: AES selected a fixed polynomial which is facilitating to calculate. The polynomial is c(x)=03x3+01x2+01x+02.

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \end{bmatrix} \begin{bmatrix} s00 & s01 & s02 & s03 \\ s10 & s11 & s11 & s13 \\ s20 & s21 & s12 & s23 \end{bmatrix} = \text{Result matrix of column mix}$$

(4). Key plus

B2	10	C1	AC
38	62	6E	E7
75	80	2C	5B
4A	9C	23	80

$\oplus$

88	8D	FE	FE
34	55	37	62
48	71	74	7D
FA	AC	9D	AF

$=$

3A	9D	3F	52
0C	37	59	85
3D	F1	58	26
B0	30	BE	2F

(5). Key Expansion: the key to be calculated as the basic unit of bytes is expressed by a matrix of four lines.

Round key length=block length *(Round Nr+1)

Decryption process

(1). Inverse byte substitution: Like the byte substitution, Inverse byte substitution search each byte though the table.

(2). Inverse row displacement: In contrast with Row displacement operation.

(3). Inverse column mix: almost the same as column mix operation, but inverse column mix has its own polynomial. The polynomial is d(x)=0Bx3+0Dx2+09x+0E.

(4). Key plus: the same as key plus operation in encryption process.

Summaries

With the rapid development of Internet technology, the data of the users' information have raised up largely. It makes cloud storage render a portable data storage service to domestic consumers gradually. In this paper, a cloud storage system has been designed, and we use AES encryption algorithm to implement the security mechanism of the system.

References

[1]. C.Wang,Q.Wang,K.Ren and W.Lou. "Ensuring data storage security in cloud computing" in Proc. Of IWQoS'09, Charleston, South Carolina, USA, 2009.

[2]. Paul Biggar , Edsko de Vries , David Gregg, A practical solution for scripting language compilers, Proceedings of the 2009 ACM symposium on Applied Computing, March 08-12, 2009

[3]. Elbirt A.J., Yip W., Chetwynd B., Paar C.: An FPGA Implementation and PerformanceEvaluation of the AES Block Cipher Candidate Algorithm Finalists, Third Advanced Encryption Standard (AES3) Candidate Conference, New York, 2000.

[4]. Gaj K. and Chodowiec P.: Comparison of the hardware performance of the AES candidates using reconfigurable hardware, Third Advanced Encryption Standard (AES3) Candidate Conference, New York, 2000

[5]. G. Ateniese, R. Burns, R. Curtmola, J. H. amd Lea Kissner, Z. Peterson, and D. Song. Provable data possession at untrusted stores. In Proceedings of the ACM Conference on Computer and Communications Security, 2007