Study on Strategy of Cloud Computing Data Storage Security

Sha Liu[1], Shuhua Zhu[2]

[1]School of Information Science and Technology, Jinan University, Guangzhou, China

[2]Network & Educational Technology Center, Jinan University, Guangzhou, China

shaliu@163.com

Keywords: Cloud Computing; Data Security; Trusted Platform Module

Abstract. With the popularization and application of cloud computing services, cloud storage has become a typical representative of cloud computing services. But meanwhile, we must also recognize that the problem of storing data in a cloud environment can be brought to us. In this paper, we propose a cloud data storage security solution based on security chip. Combined with the feature of trusted cloud computing, we have put forward the corresponding solution ideas and methods, including user registration, root key and root certificate generation, identity authentication and data storage and transmission security protocol.

Introduction

The primary purpose of data security is to protect the data in network environment or large systems from malicious tampering, destroying, disclosing and stealing. For emerging cloud computing technology, the security risks it faces includes computing service own security risks, and cloud platform user data security risks as well. With the popularization and application of cloud computing services, cloud storage has become a typical representative of cloud computing services. But meanwhile, we must also recognize that the problem of storing data in a cloud environment can be brought to us.

When users store data in personal devices, they have the highest operating authority for the data and are responsible for ensuring the security of the data. However, when users store the data in cloud platform, they have to lose control over their own data, because the cloud service providers have their own data services and security policy. Currently, most of the cloud service providers have introduced data security services, but the effect is not ideal. In addition, the recurring equipment failure, service delay, data loss and authentication error have caused a crisis of confidence in cloud computing services. One of the key factors driving the popularity of cloud computing is reliability, so we focus on data storage security in cloud computing platform.

Cloud Data Storage Security Solution Based on Security Chip

In this paper, we propose a cloud data storage security solution based on security chip. This solution starts with root of trust for measurement of TPM (trusted platform module), to conduct integrity measurement of platform components. In the boot process, in order to ensure the credibility of the cloud computing platform, the launched software requires to be measured by cloud server with related trusted computing technology. In order to achieve the integrity of platform identity protection, the cloud server would take the trusted report root of TPM as the unique identity of the platform; by the trusted storage root of TPM, the platform can achieve key management and secure transmission and storage of data in cloud computing environment.

The cloud data transmission and storage security system contains three functional entities of trusted CA server, trusted cloud server and client. The trusted cloud server is equipped with TPM security chip, to build a trusted cloud computing environment with security features of TPM. The overall solution of the cloud data transmission and storage security system is shown as Figure 1:

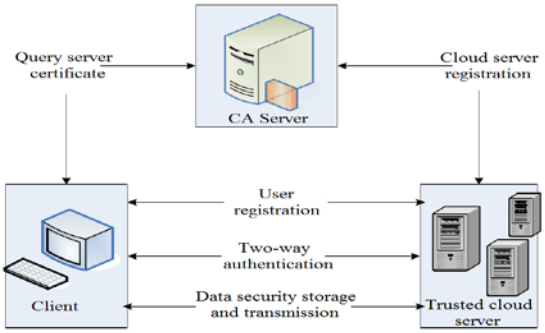

Fig.1 Overall solution of the cloud data transmission and storage security system

As a trusted third party, there is built-in TPM chip in the trusted CA server. CA is responsible for issuing, checking, undoing and other operations for certificate management. Virtual machine in cloud server generates the identity authentication key AIK, and then is registered with the CA; after CA server audit, identity certificate AIK is issued to cloud server.

There is also built-in TPM chip in trusted cloud server. With vTPM technology, each virtual machine instance of the operating system can directly call the functions of encryption, secure storage, authentication and integrity reports of TPM. The trusted cloud server is registered in CA center and then obtain AIK identity certificate. Trusted cloud server provides users with related services, and only after two-way identity authentication with the client, the client can properly access to corresponding the cloud services.

Data Storage and Transmission Process

The data storage and transmission process is shown as Figure 2:

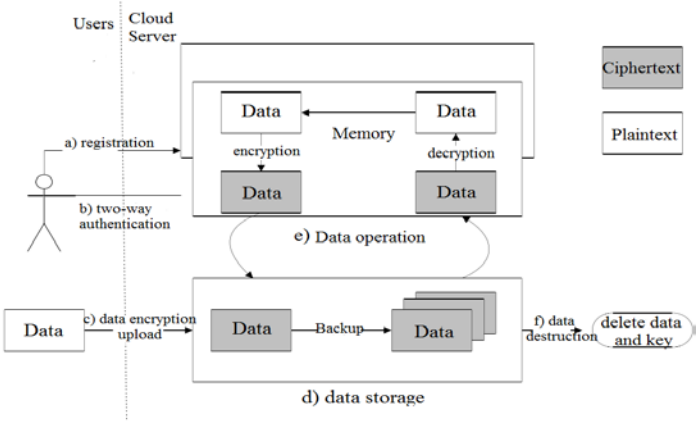

Fig.2 Data storage and transmission process

First, users need to complete the registration in the cloud platform; second, users need to complete mutual authentication with cloud server, and obtain communication key; third, users use the communication key to encrypt the messages, and meanwhile carry out processing of the application and data in accordance with the designed data protocol; after uploading to the cloud, VMM will manage the corresponding key; in addition, users can delete the application or data in the cloud.

User registration. To obtain services provided by cloud environments, firstly users need to be legitimate users of the system. User registration contains two main processes: users send registrations; cloud server issues registration information to the user. Specific steps of user registration are shown as Figure 3:

a) When a user requests to the cloud server for registration, user select an identity (ID), password (PW) and a random number n, and generate a pair RSA asymmetric key $\{PK_u, SK_u\}$, and calculate h (PW $\oplus$ n); then send $\{ID, h (PW \oplus n), PK_u\}$ to cloud server S;

b) When cloud server receives the user registration message, firstly calculate $R=h(ID||x) \oplus h(PW \oplus n)$. In addition, system initiates encryption operation on {R} with user public key PK_u, and finally cloud server issues registration information to the user, which is the encrypted cipher text;

c) When user receives the request, he can decrypt the cipher text with user private key SK_u, and get R; then user import the ID, SK_u, n and R into the smart card. The smart card information is {ID, SK_u, R, n}. Afterwards users do not need to remember n any longer.

Thus, user registration in cloud server system is completed.

Generation of trusted CA server root key and root certificate. Before the related operations, the trusted CA server needs to generate root key and root certificate.

a) Generation of CA server root key. In CA server, the security chip generates asymmetric keys used for signing and verification. The root key is used to issue and validate all user identity certificates.

b) Generation of CA server root certificate. Trusted CA server takes the root key self-signed certificate as its root certificate. The main fields of trusted CA server root certificate mainly include root certificate serial number, root certificate validity period, server identity, server public key, server self-signature, etc.

Two-way identity authentication. Before data interaction, user and cloud server should get the communication key, so they need to complete two-way identity authentication. Only by establishing secure communication with the virtual monitor on the cloud server, users will rest assured that the personal information and private data uploaded to the cloud server. The specific process of identity authentication is as follow:

1) User sends authentication request to cloud server;

2) Cloud server processes user login request, and verifies the user's identity;

3) Cloud server generates ACK, and meanwhile send identity authentication of cloud service platform;

4) Users handle the ACK, measure the integrity of the platform, and then obtain the communication key.

Thus, users complete the two-way identity authentication, and then successfully land the cloud server to obtain services provided by the cloud server. In subsequent interaction process, users use K_{us} to handle the communication information.

Data storage and transmission security protocol. In this system, we mainly focus on the security of application and user data. After the user and trusted cloud server completing the authentication, it get the communication key K_{us}, to ensure the security of data storage. The system generates identity key pair for every application, that is, PK_{app}/SK_{app}.

Firstly, users need to submit the registration request of application to the virtual machine manager, including PK_u, register command, main program name, PK_{app}, and then encrypt with session key K_{us}, as shown in Figure 4-(a).

Then system generates an AES symmetric key, as shown in Figure 4-(b). With the AES symmetric key, system encrypts the data and executable text. Meanwhile, to ensure the security of AES key, attach AES key to the end of the application after encryption, and send the encrypted file and key to server.

Because of the system maintenance, upgrading and the occurrence of disasters, we need to backup the data for multiple times. Since the data is in the form of a text message in cloud server platform, operations in system will not pose a threat to the privacy of the data.

In the process of application execution, other processes and OS are not accessible to the application’s private run space of memory. In this process, VMM acts as a bridge between the OS and the users. When copy the data from OS to private memory space for user programs, VMM will conduct decryption operation on data; when copy the data from user program memory space to OS, such as writing data to disk, VMM will use the symmetric key of application to encrypt the data. The user data is storage in the form of ciphertext, so as to ensure the security of user data.

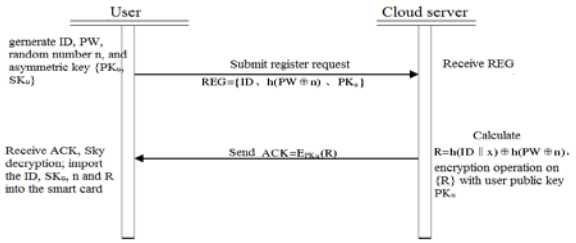

Fig. 3 Specific steps of user registration

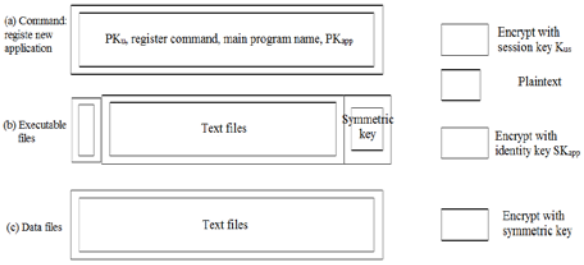

Fig. 4 Specific steps of user registration

REFERENCE:

[1] Wang Q, Wang C, Li J, et al. Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing[J]. Lecture Notes in Computer Science, 2009, 22(5):355-370.

[2] Wang C, Wang Q, Ren K, et al. Ensuring data storage security in cloud computing[C]// in Proc. of IWQoS'09. 2009:1 - 9.

[3] Wang C, Wang Q, Ren K, et al. Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing[C]// INFOCOM, 2010 Proceedings IEEE. IEEE, 2010:1 - 9.

[4] Kumar, Pranav, Subramanian, Ramanathan, Selvam, D. Thamizh. An Efficient Distributed Verification Protocol for Data Storage Security in Cloud Computing[C]// Advanced Computing, Networking and Security (ADCONS), 2013 2nd International Conference on. IEEE, 2013:214 - 219.

[5] Yawale N M, Gadicha V B. A Result Analysis on Privacy-Preserving Public Auditing System of Data Storage Security in Cloud Computing through Trusted TPA[J]. International Journal of Computer Science & Information Technolo, 2014.

[6] Danan Thilakanathan, Chen S, Surya Nepal, et al. Secure Multiparty Data Sharing in the Cloud Using Hardware-Based TPM Devices[C]// Cloud Computing (CLOUD), 2014 IEEE 7th International Conference on. IEEE, 2014:224-231.