Research on Key Technology of Authentication and Key Negotiation in Cloud Computing Environment

Wang Linjing, Zhao Chunxia

Henan University of Traditional Chinese Medicine,Zhengzhou 450008,China

Xuexi123@163.com

Keywords: Cloud computing environment; Key agreement; Exchange protocol; Cross cloud authentication; Embedded watermark.

Abstract. Due to the complexity of cloud computing environment, cloud computing in the process of information security certification not only requires the server identifying user information, but also identifying authenticity of user authentication server, which can realize two-way authentication between server and user authentication. Based on this, a cross cloud authentication scheme based on the three party password authentications key exchange protocol (3PAKE) is proposed, which uses homomorphism authentication protocol and uses a symmetric encryption algorithm to improve the security and efficiency of data. In order to verify the validity and reliability of the protocol verification algorithm, through the embedded cloud watermark in the user image information, this paper verifies the protocol algorithm, discovered by the encryption and decryption operation, homomorphism symmetric protocol algorithm can effectively encrypt the image, and the extracted decrypt feature is greater than 50%, which can be reduced to obtain more clear image, and the protocol algorithm is accuracy and high reliability.

Introduction

In recent years, cloud computing has become a new model of IT resource use. This model has the characteristics of strong computing power, high reliability, low cost and assigning resources according to need [1-3]. Therefore, it is highly valued by academia and industry. The major problem of cloud computing services in the development process is security. The reason why a lot of people do not choose the cloud service system is they are concerned about the cloud environment is not able to effectively protect data security and personal privacy, while the cloud environment system is also frequently appeared cloud security incident. In the cloud computing environment, data transmission is one of the most frequent operations and is the most vulnerable to be triggered attack in the security problem [4]. To ensure the security of data transmission based on the authentication, it needs to encrypt and decrypt the data to ensure the safety of using cloud platform.

Security Issues of Cloud Computing Data

The key feature of cloud computing environment is that all services are provided through the network, the user's data is stored in the cloud, and the results are returned to the client through the network. Cloud computing environment is a new service model, because its resource is distributed, and users can share between computing and storage resources, so the user can easily generate malicious attacks, the user's data is easily stolen or tampered [5-6]. Cloud computing environment is mainly faced with three aspects of risk:

Security risk of data transmission. Under normal circumstances, the enterprise will save a large number of private data in cloud, such as customer information, financial situation and key business processes [7]. The enterprise will face three problems when the data is transferred to cloud service providers, the first is whether the data is encrypted in the transmission, and even after being stolen it can’t be effectively reduced; the second is how to ensure that the service provider doesn’t leak data; the third is when the cloud service providers store data, how to ensure the user's authentication authority that companies can access to storage data.

© 2015. The authors - Published by Atlantis Press

Security risk of data storage. Data storage is the most important part of cloud services, data storage location, data isolation level and data storage are security risks [8] . It means whether there is a security risk when cloud service providers storing resources, whether the data will be effectively isolated after data encryption, ,whether there is valid backup so you can restore the storage data in case of a major accident.

Security risk of data audit. In the actual work process, in order to ensure the accuracy of the data, it will introduce the third party to audit the data. Therefore in the cloud computing environment, cloud service providers need to ensure that the data doesn't generate the risk on other enterprises when helping the third party certification body to audit data security [9]. In the audit process, it needs to ensure that the audit institution doesn't disclose data.

Key Technology of Cloud Computing Environment Security Authentication

In cloud computing environment, main function of cloud computing is realized by the virtual computing [10]. For security authentication of virtual computing, it can introduce trusted cloud framework, including the trusted root and trusted transfer, to achieve the measurement and verification of virtualization computing layer and application service layer, and the structural framework is as shown in Figure 1.

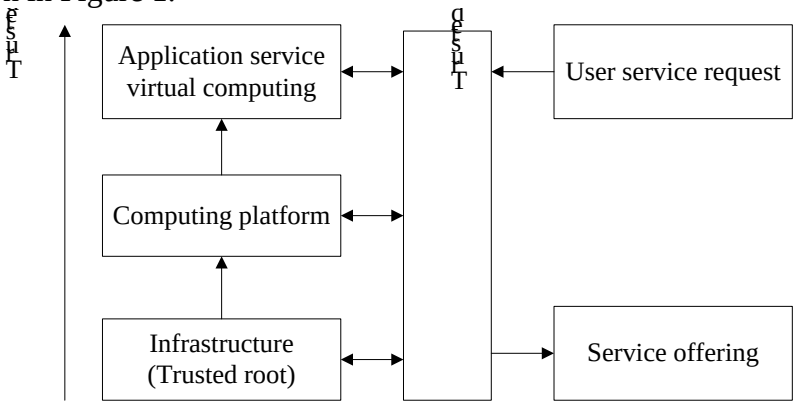

Fig. 1 Trusted cloud environment security authentication framework

Figure 1 represents a trusted cloud environment security authentication framework. The first is from the trusted root to identify the credibility of cloud computing platform, virtual computing layer and cloud service providers to ensure the credibility of the cloud environment, and then using the 3PAKE program to achieve cloud user registration.

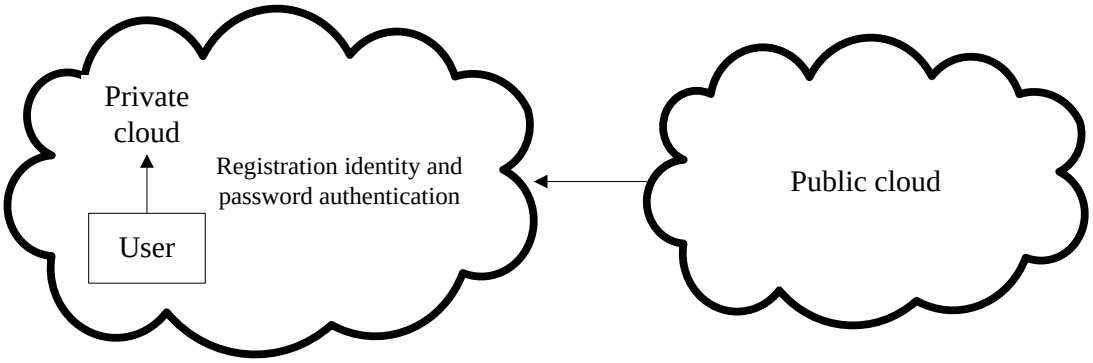

Fig. 2 Cloud computing environment security registration phase

In order to protect the security of cloud computing environment data, this paper uses 3PAKE cross cloud authentication scheme, and 3PAKE key agreement has two authentication parties, including public and private cloud [11]. Public cloud and private cloud use two-way authentication method, a certification server corresponding to a private cloud authentication server. When the user needs to access the public cloud, the operation is as shown in Figure 3.

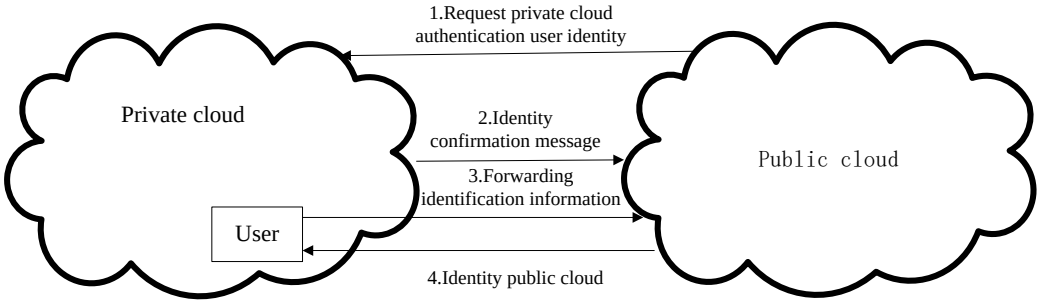

Fig. 3 Cloud computing environment security certification stage

Figure 3 shows in cloud computing environment security authentication stage it mainly consists of four steps: the first is public cloud receives user authentication request, public cloud requests the private cloud to help achieve two-way authentication between users, and then private cloud identifies if user information is legal. If it is Ok, it will be passed and give confirmation information, and then the user send the identified information according to the authentication information to complete two-way authentication process. According to key agreement, one of users and public generates the key; the other verifies and gets the key, so as to achieve secure communication.

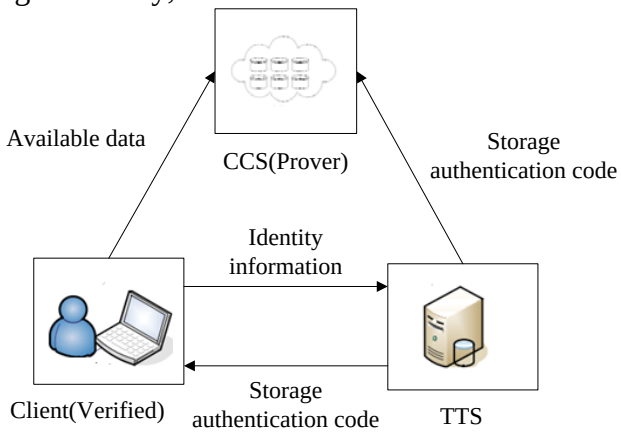

Fig. 4 Storage architecture security design

Figure 4 shows the security design of the storage structure. Storage structure mainly includes three categories of entities, including client, trusted third party and cloud storage server (CSS). TT means the credibility of the media between Client and CSS, which can be stored with user information to verify the user's ID, CSS is mainly used to store a variety of data to ensure the integrity of data storage.

Cloud Computing Environment Key Agreement and Encryption Algorithm

The key of the cloud computing environment uses full-state encryption algorithm. Assuming that the encryption operation is *E*, the text of transmission data is *m*, after encryption it is *e*, decryption operation is *D*, so it can get

$$e = E(m) \qquad m = D(e). \tag{1}$$

Doing operation on test *f*, constructing *F* for *E*, so it can get:

$$F(e) = E(f(m)). \tag{2}$$

E is homomorphism encryption of *F*. The encryption process can do the direct operation on the cipher text without it. In order to improve the security and computational efficiency of data, on the basis of fully homomorphism, countermeasure encryption is introduced, and the algorithm can guarantee the data theft can't reduction. Symmetric homomorphism encryption algorithm is divided into the following steps:

Parameter selection: assuming that the encryption parameter is *q* and *r*, $r \sim 2^n, p \sim 2^n, q \sim 2^n$;

Key: if the key is an odd number *q*;

Encryption: text is encrypted, the process of encryption is $c = pq + 2r + m$, so as to get the cipher text;

Decryption: $m = (c \mod p) \bmod 2$;

Correctness verification: because $pq \geq\geq 2r + m$, so $(c \bmod p) = 2r + m$, $(c \bmod p) \bmod 2 = (2r + m) \bmod 2 = m$. Take addition as an example, suppose the two cipher text file is $c_1 = pq_1 + 2r_1 + m_1$ and $c_2 = pq_2 + 2r_2 + m_2$, so $c_1 + c_2 = p(q_1 + q_2) + 2(r_1 + r_2) + m_1 + m_2$. So it only needs to meet $2(r_1 + r_2) + m_1 + m_2$ is smaller than p, so $(c_1 + c_2) \bmod p = 2(r_1 + r_2) + m_1 + m_2$. That satisfies the condition of the encryption.

Cloud Computing Environment Image Encryption and Decryption Test

In order to verify the reliability of cloud environment authentication and key agreement, this paper uses the method of watermark droplets to test the protocols and algorithms. Firstly it selects a pixel matrix $m*n$ without watermark, each pixel gray value is between [0-255]. The image before and after adding watermark is as below:

Fig.5 Image before and after adding watermark

Figure 5 is the image before and after adding watermark. In order not to damage the user's data, the image data is embedded cloud watermark, and watermarking can be used as statement of copyright issues. The cloud droplet embedding using fully homomorphism symmetric encryption algorithm and the process is shown in Figure 6.

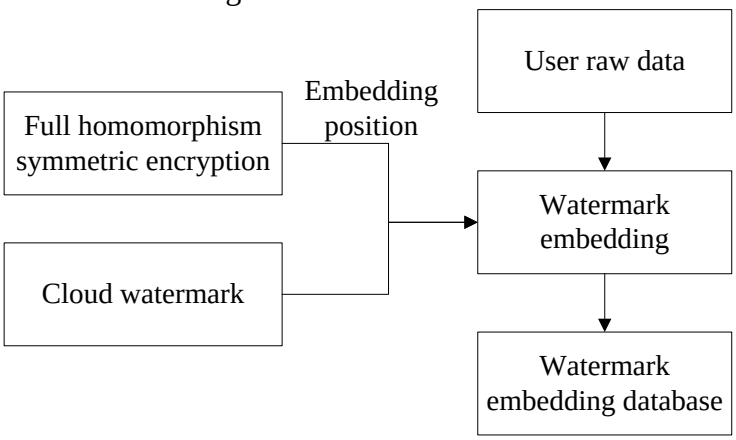

Fig. 6 The cloud watermark embedding process

Figure 6 shows the cloud watermark embedding process. This paper uses the fully homomorphism symmetric confidentiality agreement algorithm to embed the cloud watermark in the original image, after that it forms the watermarking database, and it can use decrypt to extract and reduce the data.

Fig. 7 Image effect with different recovery ratio

Figure 7 shows image effect with different recovery ratio. From the image it can be seen, using human image identification ability, when the recovery ratio of the data is more than 50%, the watermark image is clear, so as to verify the validity and reliability of the algorithm.

Summary

Based on the full homomorphism and symmetric encryption algorithm, this paper proposes a cross cloud authentication scheme based on the three party password authentications key exchange protocol, which can realize the two-way authentication between the cloud server and the user, improve the security and efficiency of user data. This paper uses embedded cloud watermark in the user image data to verify the validity and reliability of fully homomorphism symmetric encryption protocol algorithm. Through the test it can be found the protocol algorithm can effectively embed cloud watermark in the image. Using human image identification ability, when data extraction recovery ratio is more than 50%, the watermark image display more clearly and the decryption is better.

References

[1] H. Wu, S.G. Yan, S.X. Xue. Design and implementation of Ethernet data transmission system based on W5300. Electronic engineering design, 2014, (9)13: 92-94.

[2] M.X. Yao. Research and implementation of encryption algorithm in network information security. Computer knowledge and technology, 2013, 12(28): 25-29.

[3] L.S. Liu. Encryption algorithm based on RSA. Computer knowledge and technology, 2014, 3 (21): 20-23.

[4] Y. Liu. Enterprise private cloud platform construction technology research. Computer age, 2014, 6(4): 38-41.

[5] Y. Ouqun, K. Zhao. Application of cloud software platform in the multimedia classroom. Chinese information technology, 2013, 2(16): 242-243.

[6] K. Lu. Embedded media player design based on STM32F103VCT. Journal of Hunan Industrial Vocational and technical college, 2013, 18(5): 34-39.

[7] Y.F. Pu, W. Zhang, S.H. Teng, H.L. Du. The collaborative network intrusion detection based on decision tree. Journal of Jiangxi Normal University: Natural Science Edition, 2013, 34(3): 302-307.

[8] H.Q. Lu, F. Wang, Y.S. Song et al. Damage assessment system based on combat simulation. Journal of PLA University of Science and Technology: Natural Science Edition, 2013, 10(2): 139-143.

[9] H.M. Wang Y. Zhang. Research on the model of the joint operation simulation situation. Journal of system simulation, 2014, 20(15): 4186-4188.

[10] Z.M. Xu, J. He. Design and implementation of battlefield situation 3D graphics simulation. Computer application, 2014, 3(29): 313-316.

[11] C. Yang, C.J. Cao, J.F. Ma. GM composition security authentication protocol for wireless mesh networks. Xi'an University of Electronic Science and technology, 2013, 3 (5): 514-517.