Enterprise private cloud file encryption system based on tripartite secret key protocol

Xinxian Li[1, a], Weiqin Li[2, b], Daisong Shi[2, c]

[1]NanYang Medical College, Nanyang, 473061, China;

[2]Southwest Petroleum University, Chengdu, 610500, China

[a]email:sollor@126.com, [b]email:nengdee@163.com,[c]272529426@qq.com

Keywords: private cloud; tripartite secret key protocol; authentication; safe

Abstract. More and more enterprises have their own private cloud computing center or the data center to optimize operation and save money. In order to protect sensitive company data, a secure and efficient certificate less tripartite key agreement protocols was introduced into the authentication of the enterprise private cloud file system encryption. The analysis results show that this scheme high security and efficiency compared with the traditional scheme. This solution solved the main security and efficiency problems in large scale application environment.

Introduction

With the rapid development of network technology and the popularity of cloud computing technology, more and more enterprises, universities and research institutions recognized. In the enterprise private cloud encryption and authentication of a file system, foreign earliest uses is the user name and password of the password authentication, the authentication mode is simple, fast and does not require a digital certificate and other ancillary equipment. But there are serious security vulnerabilities, prone to external leakage and password guessing problem, not up to the requirements for safety enterprise private cloud. Multi factor authentication key and authentication ring pattern will be combined to propose a "one-time password"[1], although this scheme greatly improves the strength of authentication, but also increases the cost, also did not complete the identity authentication of the clouds [2].Majority of the domestic cloud products is a digital certificate authentication way based on a strong security authentication of multi factors of these digital certificate, solves the defect of cloud identity, but this kind of authentication scheme of authentication efficiency is low, and there will be trouble certificate management[3]. In this paper we according to the overall framework and authentication features private cloud encryption file system, we proposed an efficient identity aggregate signature private cloud encryption file system based authentication scheme to replace the authentication scheme based on digital certificate.

No certificate-based tripartite key agreement protocol

Key agreement protocol, which allows two or more users to create a shared secret key in a public network, it is the most basic public key cryptography. Reference [4] presented the first three party key agreement protocol, this protocol has higher efficiency, realized the key negotiation between three entities, but it is not authenticated. According to the literature [1] identity based encryption scheme, proposed an ID based three party authenticated key agreement protocol is new, this protocol solves the authentication problem of three party key agreement process, but the existence of key escrow problem.

Here, literature [3] presented efficient certificate less three party key agreement protocol, the key generation process certificate less three party key agreement protocols specific implementation of the agreement process shown in Fig.1.

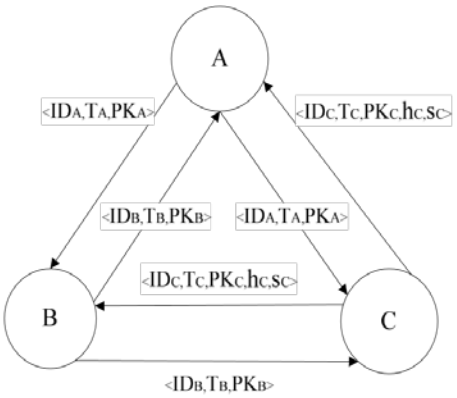

Fig.1. An information exchange process diagram tripartite agreement

$ID_{A,}$ ID_B and $ID_{C\ are}$ user A, B, C identities, they will submit their identity information to the key generation center, to generate some of their own private $D_{A,}$ $D_{B,}$ *and* $D_{C.}$ PK_A , PK_B and PK_C are the private keys for each of user A, B and C. T_A,*TB*, *TC* is the secret random number selected by each of user A, B and C.<*hc*, s_C> is the signature of user C.

Tripartite secret key agreement based enterprise private cloud Encrypting File System Authentication Mechanism

Aggregate signature of the above-mentioned proposed enterprise private cloud Encrypting File System certification programs, though there is a high efficiency and safety, but did not overcome the key escrow problem. To solve this problem while improving enterprise private cloud Encrypting File System certified strength, an efficient tripartite key agreement protocol without certificate authentication enterprise private cloud be applied to encrypt the file system[5], so we can overcome key Hosted problem. The real mutual authentication between EES and, after analysis of the program compared to the traditional scheme has a good performance. EES tripartite key agreement and authentication process shown in Fig.2.

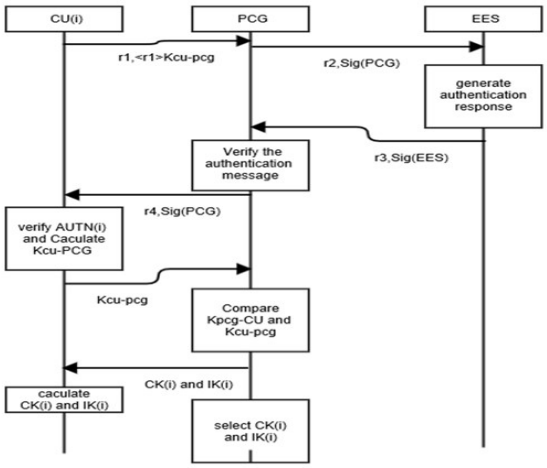

Fig.2. is based on tripartite key agreement of the certification process

Security Analysis

Security Analysis of certification scheme

1）The mutual authentication between the communicating entities

In the protocol, the certification between CU and PCG is through the mechanism of message authentication codes and signatures together to achieve. CU uses the authentication data request message and the authentication code, the shared key<r1>$K_{CU\ PCG}$ and <r4> $K_{PCG\ CU}$ to verify the identity between them using the signature.

2) Registration message security protection

PCG calculates the value of r1 <r1> $_{KCU\ PCG}$ using the received message and the shared key authentication code , if it is same to the received message authentication code<r1> $K_{PCG\ CU}$, that is to say that r1is not changed during transmission. In the same way, MN uses the shared key with FA to calculate<r4> $K_{PCG\ CU}$, and compares it with the received message authentication code <r4> $K_{CU\ PCG}$. Between PCG and EES, EES and CU, the integrity of the message is to be guaranteed with the public key of the digital signature.

3) Freshness of registration message guarantee

Freshness of messages between CU、PCG and EES is to be guaranteed by a random number. CU sends requesting authentication data with the addition of a random number *Randi* ( ), PCG will sending authentication response appending a random number generated by itself. If the random number received is not same to that it sent, the authentication fails. Therefore, the protocol can guarantee freshness of each message sent between CU、PCG and EES.

4) Confidentiality guaranteed message

Confidentiality protection of the message is encrypted by the key to achieve. CU will use $K_{CU\ PCG}$□ to generate a message authentication code during it sending a registration request message. When the authentication request arrives to PCG, it uses their private key to decrypt, and other communication entity cannot get the message as they have no the private key. Similarly, only the specific CU can obtain the message sent by PCG，.

Comparison of the certification scheme

Authentication of the program implemented include:

①EES to CU authentication; ② EES to PCG authentication;

③CU to EES Authentication; ④CU to PCG Authentication;

⑤PCG to CU authentication; ⑥ PCG to EES authentication.

The traditional authentication schemes only achieved①③⑤ certification, there are a security flaw and trap based on data streams targeted attacks and string lines phishing attacks, but based on aggregate signature scheme can protect the data transmission between PCG、EES and CU, so as to prevent the generation of a variety of ways to attack, so we can achieve the authentication ①②③④⑤,the tripartite key agreement authentication scheme truly achieve the tripartite mutual authentication, has a higher security.

Certified Performance Analysis

In our scheme, in this program we used two exponentiation (Ex) when generating the signature, three Hash operation (Pm), when used to verify the signature of two (Ex). The method is still used here to estimate the performance of the certification assessment.

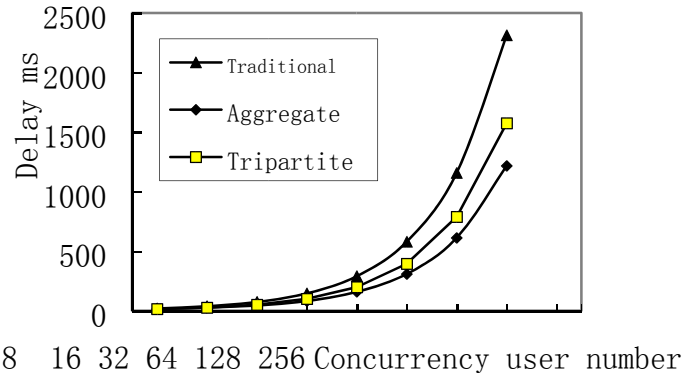

Fig.3. Concurrency user authentication delay time

As can be seen from Fig.3, when dealing with user authentication applications, though tripartite key agreement authentication scheme to verify the signature of the individual to reduce the time, few of the program when the user has certain advantages, but with the increase of users, the

polymerization Signed or have a greater advantage. This solution compared with the conventional scheme, the delay is reduced by about 25%, the program to adapt to the higher security requirements, the relatively small scale enterprises.

Conclusion

For authentication issues of enterprise private cloud encryption system, this paper based on public-key cryptosystem without certificate tripartite key agreement protocol, proposed a tripartite key agreement enterprise private cloud encryption system authentication scheme. Through the performance of enterprise private cloud Encrypting File System certification schemes analysis and summary, including security authentication mechanism analysis, analyze, compare and certified safety performance certification scheme adversary model analysis. With the increase of users, our scheme has greater advantages.

Acknowledgement

In this paper, the research was sponsored by the Nature Science Foundation of Henan Province (Project No. 201312400156326).

References

[1] Conley mountain cloud security research [D] identity-based authentication mechanism Kunming: Yunnan University, 2011.

[2] Weili Fei multiple signatures and signature research and its applications [D] polymerization Shanghai: Shanghai Jiaotong University, 2012.

[3] JOUX A. A one-round protocol for tripartite Diffie-Hellman [C] Proceedings of the 4th International Algorithmic Number Theory Symposium (ANTS-IV), London, UK: Springer- Verlag, 2000: 385-394.

[4] SHIM K. Efficient one- round tripartite authenticated key agreement protocol from Weil pairing [J] Electronics Letters, 2003, 39 (2):. 208- 209.

[5] Argyroudis PG, Vermin R, Tiwari H, et a1 Performance analysis of cryptographic protocols on handheld devices [C] // Proc.3rd IEEE Instep on Network Computing and Applications, 2004:.. 169-174.