모바일 클라우드 컴퓨팅 환경에서 ID-기반 키 암호화를 이용한 안전한 데이터 처리 기술★

천은홍* · 이연식**

요 약

모바일 클라우드 컴퓨팅 시스템은 일반적으로 데이터 보호와 상호 인증을 위하여 공개키 암호화 기법을 사용하고 있는데 최근 전통적인 공개키 암호화 기술의 변형인 ID-기반 암호화(IBC)가 주목받고 있다. IBC의 증명서-무통제 접근은 클라우드 환경의 동적인 성격에 더 적합하지만, 모바일 장치에 대하여 처리 오버헤드를 최소화하는 보안 프레임워크가 필요하다. 본 논문에서는 모바일 클라우드 컴퓨팅에서의 계층적 ID-기반 암호화(HIBE)의 사용을 제안한다. HIBE는 사용자 인증과 개인키 생성 등의 권한을 위임하여 최상위 공개키 생성기의 업무량을 감소시킬 수 있으므로 모바일 네트워크에 적합하다. 모바일 클라우드 시스템에서 ID-기반 인증과 ID-기반 신분확인 기법을 제안하고, 또한 안전한 데이터 처리를 위한 ID-기반 인증 스킴에 대하여 기술하였다. 제안된 스킴은 단방향 해쉬 함수와 XOR 연산으로 설계하여 모바일 사용자를 위한 저 계산 비용을 갖는다.

A Secure Data Processing Using ID-Based Key Cryptography in Mobile Cloud Computing

EunHong Cheon* · YonSik Lee**

ABSTRACT

Most mobile cloud computing system use public key cryptography to provide data security and mutual authentication. A variant of traditional public key technologies called Identity-Based Cryptography(IBC) has recently received considerable attention. The certificate-free approach of IBC may well match the dynamic qualities of cloud environment. But, there is a need for a lightweight secure framework that provides security with minimum processing overhead on mobile devices. In this paper, we propose to use hierarchical ID-Based Encryption in mobile cloud computing. It is suitable for a mobile network since it can reduce the workload of root Public Key Generators by delegating the privilege of user authentication and private key generation. The Identity-Based Encryption and Identity-Based Signature are also proposed and an ID-Based Authentication scheme is presented to secure data processing. The proposed scheme is designed by one-way hash functions and XOR operations, thus has low computation costs for mobile users

Key words : Mobile Cloud Computing. Identity Based Cryptography, Identity Based Authentication

접수일(2015년 8월 21일), 게재확정일(2015년 9월 14일)

★ 본 논문은 2013년도 정부(교육부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임 (13A13907331)

* 우석대학교 컴퓨터공학과
** 군산대학교 컴퓨터정보공학과

1. Introduction

The hottest wave in the IT world has now been the potential growth of Mobile Cloud Computing(MCC). Securing data in Mobile Cloud have become more important in the recent days because of increasing usage of mobile devices with the Internet. There are numerous challenges existing in the field of MCC, including data replication, consistency, limited scalability, unreliability, unreliable availability of cloud resources, portability, trust, security, and privacy[1]. Nowadays, a variant of traditional public key technologies called Identity-Based Cryptography[2] has recently received considerable attention. Through IBC, an identifier which represents a user can be transformed into his public key and used on-the-fly without any authenticity check. The potential of IBC to provide greater flexibility to entities within a security infrastructure and its certificate-free approach may well match the dynamic qualities of cloud environment. In other words, it seems that the development of IBC may offer more lightweight and flexible key usage and management approaches within cloud security infrastructures than traditional PKI does. The application of IBC in cloud computing is an emerging and interesting area.

In this paper, by adopting Identity-Based Cryptography in mobile cloud computing, we present a hierarchical architecture for mobile cloud computing first, this potentially offers a more lightweight key management approach. Then, Identity-Based Encryption and Identity-Based Signature are proposed. Finally, an authentication protocol for mobile cloud computing is presented base on the Identity-Based Cryptography. The rest of the paper is organized as follows. In Section 2, we introduce related solutions in mobile cloud computing and security problem. Section 3 presents the architectures for the mobile cloud computing, and the Identity-Based Cryptography, at the end of the section we give our proposal to the security of mobile cloud computing. Finally, conclusions and directions for future research are identified in Section 4.

2. Related Work

2.1 Security in MCC

Mobile cloud computing is a combination of mobile networks and cloud computing, the security related issues are then divided into two categories: Mobile network security; and cloud security[3]. Recent studies have classified mobile attacks in several categories such as: application based attacks, web-based attacks, network based attacks and physical based attacks. The cloud threats have been classified Privacy and Confidentiality, Data Integrity, Data Location and Relocation, Authentication and Data Availability.

2.2 Identity-based cryptography

Identity-based cryptography and signature schemes were firstly proposed by Shamir[2]. Recently hierarchical identity-based cryptography has been proposed in [4,5] to improve the scalability of traditional identity-based cryptography scheme. Nesrine and Aymen proposed a cryptographic scheme for cloud storage, based on an original usage of ID-Based Cryptography[6]. Sai Krishna and Mohd.Khaja et al. proposed the implementation of data access security in cloud using the Hierarchical Identity Based Encryption[7]. Susilo et al. proposed an identity-based data storage scheme which is suitable to the cloud computing scenario as it supports both intra-domain and inter-domain queries[8]. Schridd

et al. proposed a novel identity-based cryptographic system to avoid the complexity and management problems of certificate-based security infrastructures [9].

As the same as the approach, our method is also based on Identity-Based Cryptography. In this paper, by adopting Identity-Based Cryptography in mobile cloud computing, we present a hierarchical architecture for mobile cloud computing first. Then, Identity-Based Encryption and Identity-Based Signature are proposed. Finally, an authentication protocol for mobile cloud computing is presented.

3. Secure data processing in MCC

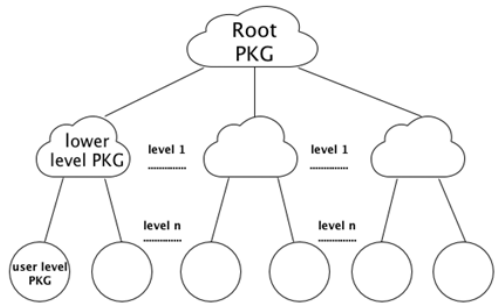
We present a hierarchical architecture, a Identity-Based Encryption and Identity-Based Signature for secure processing in MCC, and an authentication scheme for mobile cloud computing is proposed.

3.1 Hierarchical ID-based encryption for MCC

In a large network with only one Public Key Generator(PKG), the PKG will have a burdensome job. To solve this problem, HIBC can be a better choice. In a HIBC network, a root PKG will generate and distribute private keys for domain-level PKGs and the domain-level PKGs will generate and distribute private keys to the users level. HIBC is suitable for a large scale network since it can reduce the workload of root PKG by distribute the work of user authentication, private key generation and distribution to the different level of PKGs. It can also improve the security of the network because user authentication and private key distribution can be done locally.

3.1.1 Key generation in MCC

In the mobile cloud, we use two levels PKG. We define the root PKG is the PKG_{L0} and the PKGs in the private or public clouds are the PKG_{L1}. Hierarchical architectures for MCC are shown as (Figure 1).



(Figure 1) Hierarchical architectures for MCC

The root PKG_{L0} setup can be done as follow:

1) Root PKG generates G_1, G_2 and an pairing $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$
2) Root PKG chooses $P_0 \in G_1$ and $s_0 \in Z_q^*$ and set $Q_0 = s_0 P_0$
3) Root PKG chooses hash function $H: \{0,1\}^* \rightarrow G_2$

The Root PKG picks an elliptic curve, a secret s_0 and a point P_0on the curve using a random number generator. It then publishes $P_0$and s_0P_0 as the root master public key $PU_{L0_{pkg}}$, and s_0 is the corresponding master private key $PR_{L0_{pkg}}$. The root private key is only known by the root PKG.

The lower level PKG_{L1} setup can be done as follow:

For the lower level PKG_{L1}, they can use the system parameters and any user's identity to generate its public key. And every user or servers in the cloud can connect the PKGs in their cloud domain to get their private keys. For example, the PKG in a private cloud of woosuk university with the identity woosuk, its public key can be generated by the one way hash function as $PU_{woosuk} = H(woosuk)$and the root PKG can generate its private key as

$PR_{woosuk}=s_0PU_{woosuk}$. For a student user with identity st in the private cloud of woosuk university, his public key can be generated as $PU_{st}=H(woosuk//st)$, and then the private key $PR_{st}=PR_{woosuk}+PR_{woosuk}PU_{st}$.

3.2 Id-based user authentication scheme in MCC

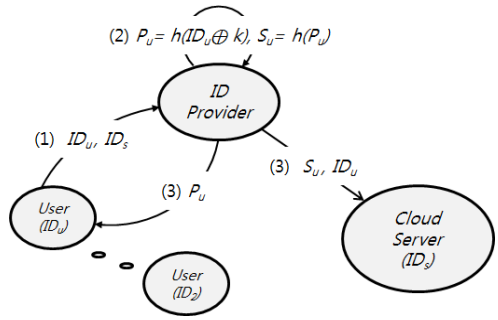
In a mobile cloud, the cloud computing system needs to provide a strong and user-friendly way for users to access all kinds of services in the system. When a user wants to run an application in the cloud, the user is required to provide a digital identity. Because the user's ID can be directly used for user authentication, the ID-based concept is very suitable for our purpose to design a new user authentication scheme for mobile cloud computing.

The authentication scheme in following steps describe the registration phase and the mutual authentication phase.

3.2.1 Registration phase

In this phase, the mobile cloud user gets the authentication information from an ID provider. We assume that the authentication information is transmitted via a secure channel. The steps of this method are shown as (Figure 2).

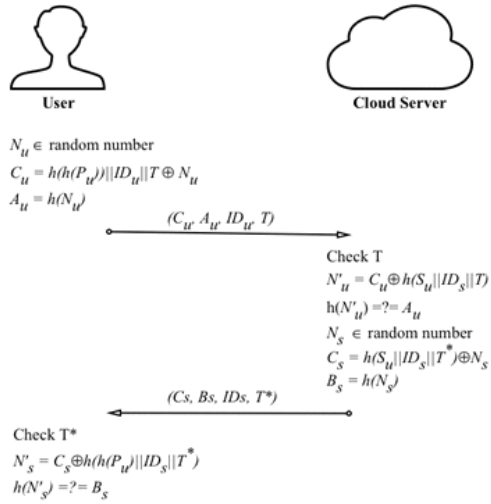
1) The mobile cloud user sends ID_u and ID_s to the ID provider for registration.
2) The ID provider uses its secret key k to compute $P_u=h(ID_u \oplus k)$ and $S_u=h(P_u)$. Then, the ID provider sends P_u to the user via a secure channel.
3) The ID provider sends ID_u and S_u to the cloud server.



(Figure 2) Registration phase of the proposed scheme

3.2.2 Mutual authentication phase

In this phase, the user logs in to the server using ID_u and P_u. Then, the cloud server can authenticate the user by ID_u and P_u. In addition, the user can also authenticate sever to use the mutual authentication. The steps of this phase are shown as (Figure 3).



(Figure 3) Mutual authentication phase of the proposed scheme

1) The user generate a random integer N_u and a timestamp T to compute $C_u=h(h(P_u))//ID_u//T \oplus N_u$ and $A_u=h(N_u)$. Then, user sends (C_u, A_u, ID_u, T) to the server.

2) The server checks T is valid. If T is valid, then the server computes $N'_u=C_u \oplus h(S_u||ID_s||T)$ and $A'_u=h(N'_u)$. If $A'_u = A_u$, Then the server can be sure that the user is legal.
3) The server generate a random integer N_s and a timestamp $T*$ to compute $C_s=h(S_u||ID_s||T*) \oplus N_s$ and $B_s=h(N_s)$. Then, the server sends $(C_s,B_s,ID_s,T*)$ to the user.
4) The user check $T*$ is valid. If $T*$ is valid, the user computes $N'_s= Cs \oplus h(h(P_u)||ID_s||T*)$ and $B'_s=h(N'_s)$. If $B'_s=B_s$, the user can be sure that the server is legal.

Through the steps, we also present the mutual authentication algorithms of the proposed scheme.

User's authentication steps:

generate a random number N_u and timestamp T
compute $C_u= h(h(P_u))||ID_u||T \oplus N_u$
send (C_u,A_u,ID_t,T) to the server.
check T^*
  if (T^* is valid){
    server computes $N'_s=C_s \oplus h(h(P_u)||ID_s||T^*)$
    $B'_s = h(N'_s)$
      if ($B'_s == B_s$) {
      the user can be sure that the server is legal }
    }

Server's authentication steps:

check T
  if (T is valid){
    server computes $N'_u = C_u \oplus h(S_u)||ID_s||T)$
    $A'_u= h(N'_u)$
      if ($A'_u == A_u$) {
      the server can be sure that the user is legal }
    }
generates a random number N_u and a timestamp T
compute $C_s= h(S_u))||ID_s||T \oplus N_s$
sends (C_s,B_s,ID_s,T^*) to the user.

According to the above steps, the proposed scheme is designed by one-way hash functions and XOR operations, so it has low computation costs for mobile cloud users. Besides, the user's authentication information is generated by the ID provider. Therefore, the proposed scheme is easily applied to multi-server environments. That is, the user can use one ID to log in to different cloud servers.

4. Conclusions

Mobile Cloud Computing is exploring vast in IT due to anywhere anytime data access. In MCC, there are still numerous challenges existing in the field of MCC, including data replication, data confidentiality and integrity. So there is a need for a lightweight secure framework that provides security with minimum communication and processing overhead on mobile devices.

In this paper, we presented a hierarchical architecture for mobile cloud computing based on IBC, this potentially offers a more lightweight key management approach and it also can restrict the key escrow problem. It is suitable for a mobile network since it can reduce the workload of root PKG by delegating the privilege of user authentication and private key generation to the different level of PKGs. It can also improve the security of the mobile network because user authentication and private key distribution can be done locally. Then, Identity-Based Encryption and Identity-Based Signature were proposed to improve data confidentiality and data integrity in mobile cloud storage systems. Finally, an ID-Based Authentication scheme were presented, the proposed scheme allows the user to log in to different cloud servers using one single ID. Thus, it is not necessary to maintain different IDs for different cloud servers. In addition, the proposed scheme has

less computation and communication costs, so it is very suitable for the cloud user who uses a mobile device to access cloud services.

References

[1] D. Zissis, D. Lekkas, “Addressing cloud computing security issues, Future Generation Computer Systems”, pp.583~592, 2012.

[2] Shamir, A, “Identity-based cryptosystems and signature schemes”, CRYPTO 1984. LNCS, vol. 196, pp. 47~53. Springer, Heidelberg ,1985.

[3] D. Huang, Z. Zhou, L. Xu, T. Xing and Y. Zhong, “Secure Data Processing Framework for Mobile Cloud Computing”, IEEE INFOCOM 2011 Workshop on Cloud Computing, IEEE, pp. 620~624, 2011.

[4] Gentry, C., Silverberg, A. “Hierarchical ID-Based cryptography.” ASIACRYPT 2002. LNCS, vol. 2501, pp. 548~566. Springer, Heidelberg, 2002.

[5] Horwitz, J., Lynn, B. “Toward Hierarchical Identity-Based Encryption.” EUROCRYPT 2002. LNCS, vol. 2332, pp. 466~481. Springer, Heidelberg, 2002.

[6] N. Kaaniche, A. Boundguiga. “ID-Based Cryptographty for Secure Cloud Data Storage” Communicating System Laboratory Saclay, 91400, France, 2012.

[7] S .K.Parsha, M .K.Pasha, “Enhancing Data Access Security in Cloud Computing using Hierarchical Identity Based Encryption(HIBE)”, International journal of scientific & engineering research volume3, issue5, May 2012.

[8] J. Susilo, Y.Mu, “Identity-based data storage in cloud computing”, Faculty of Engineering and Information Sciences, 2012.

[9] C. Schridde, T. Dornemann, E. Juhnke, B. Freisleben, M. Smith, “An Identity-Based Security Infrastructure for Cloud Environments,” 2010 IEEE International Conference on Wireless Communications, Networking and Infor- mation Security, pp. 644 ~ 649, 2010.

[저 자 소 개]

천 은 홍 (Eun-hong Cheon)

1981년 2월 광운대학교 응용전자공학과(공학사)
1985년 2월 아주대학교 전자공학과(공학석사)
1998년 8월 아주대학교 컴퓨터공학과(공학박사)
1988년 9월 ~ 현재: 우석대학교 컴퓨터공학과 교수

email : ehcheon@woosuk.ac.kr

이 연 식 (Yon-sik Lee)

1982년 2월 전남대학교 전자계산학과(공학사)
1984년 2월 전남대학교 전자계산학과(이학석사)
1994년 2월 전북대학교 전산응용공학(공학박사)
1986년 3월 ~ 현재: 군산대학교 컴퓨터정보공학과 교수

email : yslee@kunsan.ac.kr