INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 4 ISSUE 3 (2018) PAGES 3591 - 3595
RECEIVED : 15.04.2018 PUBLISHED : 20.05.2018
May 20, 2018

Cloud Revocation Authority Using Identity Based Public Key Cryptosystem And Its Applications

[1]Sowmya.L PG Scholar, Computer Science Engineering, Bharathidasan Engineering College, Natrampalli, Vellore, Tamil Nadu.

[2]R. Vasanthi , Asst Professor, Computer Science Engineering , Bharathidasan Engineering College, Natrampalli, Vellore, Tamil Nadu.

[3]A.Sudhakar, HOD, Computer Science Engineering, Bharathidasan Engineering College, Natrampalli, Vellore, Tamil Nadu.

Abstract:

Identity-based encryption (IBE) is a public key cryptosystem(encoding and decoding) and eliminates the demands of public key infrastructure(PKI) and certificate administration in conventional public key settings. Due to the absence of PKI, the revocation problem is a critical issue in IBE settings. Several revocable IBE schemes have been proposed regarding this issue. Quite recently, by embedding an outsourcing computation technique into IBE, a revocable IBE scheme with a key-update cloud service provider (KU-CSP) was proposed. However, their scheme has two shortcomings. One is that the computation and communication costs are higher than previous revocable IBE schemes. The other shortcoming is lack of scalability in the sense that the KU-CSP must keep a secret value for each user. In the article, we propose a new revocable IBE scheme with a cloud revocation authority (CRA) to solve the two shortcomings namely, the performance is significantly improved and the CRA holds only a system secret for all the users. For security analysis, we demonstrate that the proposed scheme is semantically secure under the decisional bilinear Diffie-Hellman (DBDH) assumption. Finally, we extend the proposed revocable IBE scheme to present a CRA-aided authentication scheme with period- limited privileges for managing a large number of various cloud services.

Keywords: Cloud Revocation Authority; Private Key Generator; Master Time Key; Time Update Key; Identity Key; Identity Based Encryption; Public Key Infrastructure.

1. INTRODUCTION

The PKG sends user the corresponding identity key via a secure channel. Meanwhile, the PKG must generate a random secret value (timekey) for each user and send it to the KU-CSP. Then the KU-CSP generates the current time update key of a user by using the associated time key and sends it to the user via a public channel outsourcing computation technique into IBE to propose a revocable IBE scheme with a key-update cloud service provider (KU-CSP). They shifts the key- update procedures to a KU-CSP to alleviate the load of PKG. Existing scheme also used the similar technique adopted in Tseng and Tsai's scheme, which partitions a user's private key into an identity key and a time update key. ID-based encryption (IBE) allows a sender to encrypt message directly by using a receiver's ID without checking the validation of public key certificate. In existing system misbehaving/compromised users in an ID-PKS

INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 4 ISSUE 3 (2018) PAGES 3591 - 3595
RECEIVED : 15.04.2018 PUBLISHED : 20.05.2018
May 20, 2018

setting is naturally raised. Immediate revocation method employs a designated semi-trusted and online authority (i.e. mediator) to mitigate the Management load of the PKG and assist users to decrypt cipher-text. The computation and communication costs are higher than previous revocable IBE schemes. The other shortcoming is un-scalability in the sense that the KU- CSP must keep a time key for each user so that it will incur the management load.

2. PROPOSED SYSTEM

In order to solve both the un-scalability and the inefficiency in existing scheme, we propose a new revocable IBE scheme with cloud revocation authority (CRA). In particular, each user's private key still consists of an identity key and a time update key. We introduce a cloud revocation authority (CRA) to replace the role of the KU-CSP in existing scheme.

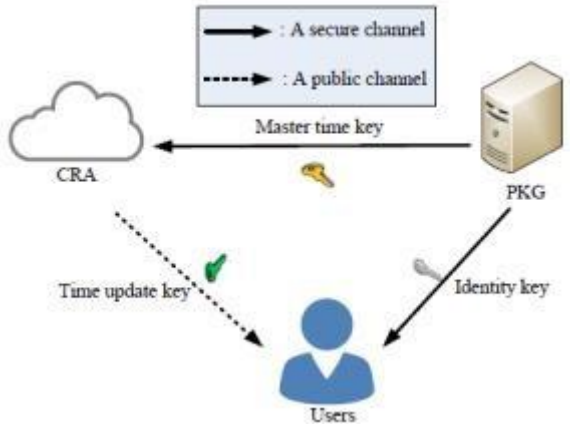

Fig.1.Architecture

The CRA only needs to hold a random secret value (master time key) for all the users without affecting the security of revocable IBE scheme. The CRA uses the master time key to generate the current time update key periodically for each non-revoked user and sends it to the user via a public channel. It is evident that our scheme solves the un-scalability problem of the KU-CSP. We construct a CRA-aided authentication scheme with period-limited privileges for managing a large number of various cloud services. The proposed scheme possesses the advantages of both Tseng and Tsai's revocable IBE scheme and existing scheme. The proposed present framework of our revocable IBE scheme with CRA and define its security notions to model possible threats and attacks. CRA-aided authentication scheme with period-limited privileges for managing a large number of various cloud services. Since a public key setting has to provide a user revocation mechanism, the research issue on how to revoke misbehaving/compromised users in an ID-PKS setting is naturally raised. In conventional public key settings, certificate revocation list (CRL) is a well-known revocation approach. In the CRL approach, if a party receives a public key and its associated certificate, she/he first validates them and then looks up the CRL to ensure that the public key has not been revoked. In such a case, the procedure requires the online. Assistance under PKI so that it will incur communication bottleneck.

3. RELATED WORK

The computation and communication costs are higher than previous revocable IBE schemes. The other shortcoming is lack of scalability in the sense that the KU-CSP must keep a secret value for each user. Cloud revocation authority (CRA) to solve the two shortcomings, namely, the performance is significantly improved and the CRA holds only a system secret for all the users. For security analysis, we demonstrate that the proposed scheme is semantically secure under the decisional bilinear Diffie-Hellman (DBDH) assumption. Revocable IBE scheme to present a CRA-aided authentication scheme with period-limited privileges for managing a large number of various cloud services. Revocation method in which each non-revoked user receives a new private key generated by the PKG periodically. A period can be set as a day, a week, a month, etc. A sender uses a designated receiver's ID and current period to encrypt messages while the designated receiver decrypts the ciphertext using the current private key, it is necessary for the users to update new private keys periodically. To revoke a user, the PKG simply stops providing the new private key for the user. It is obvious that a secure channel must be established between the PKG and each user to transmit the new private key and this would result in heavy load for the PKG. Key updates from linear to logarithmic in the number of users. However, each user's private key size is O(log n), where n is the number of users. These schemes still used a secure channel to transmit periodic private keys while no other authority shares the responsibility of user revocation. the PKG in Li et al.'s scheme and ours may also perform the revocation operations. Both the KUCSP and the CRA are designated to share responsibility for performing user revocation.

4. ANALYSIS

To reduce the sizes of both private keys and update keys, Park et al. proposed a new revocable IBE scheme by using multilinear maps, but the size of the public parameters is dependent to the number of users the secret key size of each user increases quadratic ally in the hierarchy tree wherein a low-level user must know the history of key updates performed by ancestors in the current time period, and it renders the scheme very complex Seo and Emura proposed a new method to construct a novel revocable HIBE scheme with history-free updates. Identity (id)-based public key system (ID-PKS) is an attractive alternative for public key cryptography. ID-PKS setting eliminates the demands of public key infrastructure (PKI) and certificate administration in conventional public key settings. An ID-PKS setting consists of users and a trusted third party (i.e. Private key generator, PKG). The PKG is responsible to generate each user's private key by using the associated id information (e.g. E-mail address, name or social security number). Therefore, no certificate and PKI are required in the associated cryptographic mechanisms under ID-PKS settings. In such a case, Id-based encryption (IBE) allows a sender to encrypt message directly by using a receiver's id without checking the validation of public key certificate. Accordingly, the receiver uses the private key associated with her/his id to decrypt such ciphertext. have been well studied for PKI. Indeed, researchers also pay attention to the revocation issue of ID-PKS settings. Several revocable IBE schemes have been proposed regarding the revocation mechanisms in ID-PKS settings. In 2001, boneh and franklin proposed the first practical IBE scheme from the Weil pairing and suggested a simple revocation method in which each non-revoked user receives a new private key generated by the PKG periodically. A period can be set as a day, a week, a month, etc.

INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 4 ISSUE 3 (2018) PAGES 3591 - 3595
RECEIVED : 15.04.2018 PUBLISHED : 20.05.2018
May 20, 2018

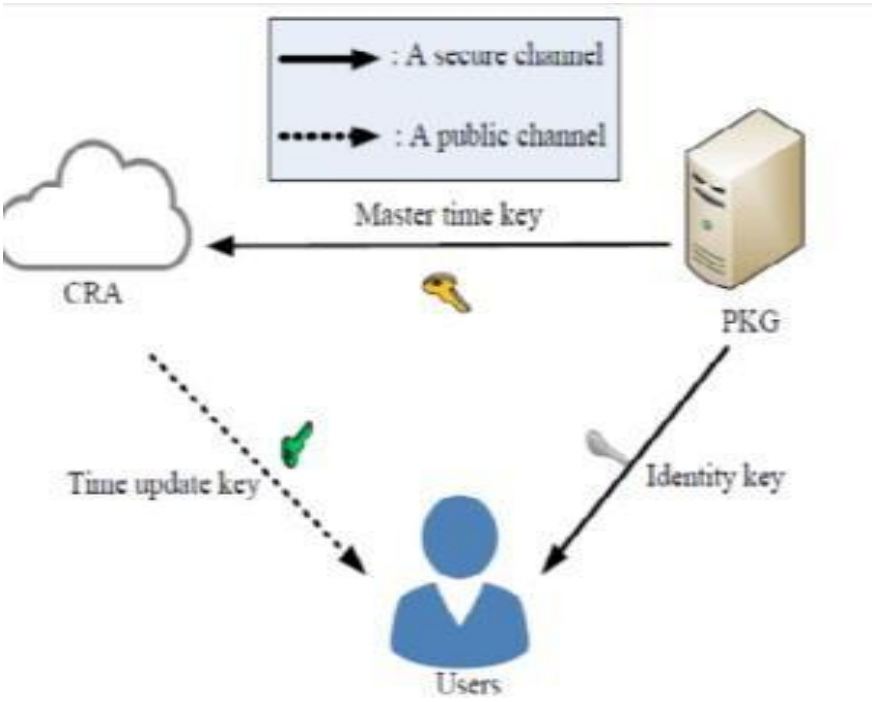

Fig.2.Proposed System

A sender uses a designated receiver's id and current period to encrypt messages while the designated receiver decrypts the ciphertext using the current private key. Hence, it is necessary for the users to update new private keys periodically. To revoke a user, the PKG simply stops providing the new private key for the user. It is obvious that a secure channel must be established between the PKG and each user to transmit the new private key and this would result in heavy load for the pkg.

CONCLUSION

We proposed a new revocable IBE scheme with a cloud revocation authority (CRA), in which the revocation procedure is performed by the CRA to alleviate the load of the PKG. This outsourcing computation technique with other authorities has been employed in Li et al.'s revocable IBE scheme with KU- CSP. In our revocable IBE scheme with CRA, the CRA holds only a master time key to perform the time key update procedures for all the users without affecting security. As compared with Li et al.'s scheme, the performances of computation and communication are significantly improved. By experimental results and performance analysis, our scheme is well suited for mobile devices. Our scheme is semantically secure against adaptive-ID attacks under the decisional bilinear Diffie-Hellman assumption. Based on the proposed revocable IBE scheme with CRA, we constructed a CR Aaided authentication scheme with period-limited privileges for managing a large number of various cloud services.

REFERENCES

[1]. A. Shamir, "Identity-based cryptosystems and signature schemes," Proc. Crypto'84, LNCS, vol. 196, pp. 47-53, 1984.

[2]. D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," Proc. Crypto'01, LNCS, vol. 2139, pp. 213-229, 2001.

[3]. R. Housley, W. Polk, W. Ford, and D. Solo, "Internet X.509 public key infrastructure certificate and certificate revocation list (CRL) profile," IETF, RFC 3280, 2002.

[4]. W. Aiello, S. Lodha, and R. Ostrovsky, "Fast digital identity revocation," Proc. Crypto'98, LNCS, vol. 1462, pp. 137-152, 1998.

[5]. M. Naor and K. Nissim, "Certificate revocation and certificate update," IEEE Journal on Selected Areas in Communications, vol. 18 , no. 4, pp. 561 - 570, 2000.

[6]. S. Micali, "Novomodo: Scalable certificate validation and simplified PKI management," Proc. 1st Annual PKI Research Workshop, pp. 15-25, 2002.

[7]. F. F. Elwailly, C. Gentry, and Z. Ramzan, "QuasiModo: Efficient certificate validation and revocation," Proc. PKC'04, LNCS, vol. 2947, pp. 375-388, 2004.