RIBE: REVOCABLEIDENTITY-BASED ENCRYPTION TO AUTHENTICATE AND MANAGING THECLOUD SERVICES

MADASU SUREKHA
PG Scholar, Dept of CSE, PACE Institute of Tech and Sciences, Vallur, Ongole, AP, India.

D ANANDAM
Assistant Professor, Dept of CSE, PACE Institute of Tech and Sciences, Vallur, Ongole, AP, India

Abstract

Public key cryptosystem removes the demands of public key infrastructure and certificate administration in conventional public key settings. Identity-based encryption is a public key infrastructure. If the absence of public key infrastructure, the revocation problem is a critical issue in Identity-based encryption settings. There are multiple revocable Identity-based encryption schemes have been proposed regarding this issue. In recent times, by inserting an outsourcing computation technique into Identity-based encryption proposed a revocable Identity-based encryption scheme with a key-update cloud service provider .This scheme has two limitations. One is that the computation and communication costs are higher than previous revocable Identity-based encryption schemes. The Second one is lack of scalability in the sense that the key-update cloud service provider must have a secret value for each user. In this Paper, I propose a new revocable Identity-based encryption scheme with a cloud revocation authority to solve the two limitations, namely, the performance is improved and the cloud revocation authority holds only a system secret for all the users. The proposed Identity-based encryption is more secure under the decisional bilinear Diffie-Hellman assumption. Finally, I extend the proposed revocable Identity-based encryption scheme to present a cloud revocation authority authentication scheme with limited privileges for managing number of cloud services.

Index Terms*—Cloud revocation authority, Identity-Based Encryption, Authentication, Public Key.*

1.INTRODUCTION

Identity based public key system [1], [2]is good method for public key cryptography. Identity based public key system eliminates the huge demands of public key infrastructure and certificate administration in conventional public key settings. An Identity based public key system setting have users and a trusted third party. The private key generator is responsible for generation of each user's private key by using the related ID information. So, no certificate and public key infrastructure are required in the related cryptographic mechanisms under ID-public key system settings. In that case, ID-based encryption allows a user(sender) to encrypt message directly by using a receiver's ID without checking the validation of public key certificate. After, the receiver uses the private key related with her/his ID to decrypt such cipher text. Since a public key setting has to provide a user revocation mechanism, the research problem is on how to revoke misbehaving/compromised users in an ID-public key system setting is naturally raised. In conventional public key settings, certificate revocation list [3] is a famous revocation approach. In the certificate revocation list approach, if a party receives a public key and its related certificate, she/he first validates them and then looks up the certificate revocation list to guarantee that the public key has not been revoked. In such a case, the procedure requires the online help under public key infrastructure so that it will incur communication holdup. To improve the performance, a number of efficient revocation mechanisms [4], [5], [6], [7], [8] for conventional public key settings have been well studied for public key infrastructure Indeed, researchers also pay awareness to the revocation issue of ID-public key system settings. a number of revocable Identity-Based Encryption schemes have been proposed about the revocation mechanisms in ID-public key system settings.

1.1 Related Work

In 2001, Boneh and Franklin [2] proposed the first Identity-Based Encryption scheme from the Weil pairing and recommended a simple revocation method in which every non-revoked user receives a new private key generated by the Private Key Generator from time to time. A period can be set as a day, a week, a month, etc. A sender uses a selected receiver's ID and current period to encrypt messages while the selected receiver decrypts the cipher text using the current private key. Therefore, it is essential for the users to inform new private keys from time to time. To revoke a user, the Private Key Generator just stops provide the new private key for the user. It is understandable that a secure channel must be established between the Private Key Generator and each user to transmit the new private key and this would result in heavy load for the Private Key Generator. In order to improve the load of the Private Key Generatorin Boneh and Franklin's scheme, Bonehet *al*. [9] proposed another revocation method, called immediate revocation. Immediate revocation method employ a selected semi-trusted and online authority to alleviate the management load of the Private Key Generator and help users to decrypt cipher text [10], [11], [12], [13]. In that a case, the online mediator must hold the shares of all the users' private keys. Since the decryption operation should involve both parties, neither the user nor the online mediator can cheat one another. When a user was revoked, the online mediator is instructed to stop supporting the user. However, the online mediator must help users to decrypt each cipher text so that it becomes a holdup for such schemes as the number of users grows extremely. Boneh and Franklin's revocation method [2], all the users must from time to time update new private keys sent by the Private key generator. As the number of users increases, the load of key updates becomes a holdup for the Private key generator. In 2008, Boldyreva*et al*. [14] proposed a revocable Identity-Based Encryption scheme to improve the key update efficiency. Their revocable Identity-Based Encryption scheme is based on the concept of the Fuzzy Identity-Based Encryption[35] and adopt the complete subtree method to decrease the number of key updates from linear to logarithmic in the number of users. In fact, by binary tree data structure of users, the scheme efficiently alleviate the key-update load of the Private Key Generator. Moreover, Identity-Based Encryptionrt and Vergnaud [16] improved the security of Boldyreva*et al*.'s revocable Identity-Based Encryption scheme by present an adaptive-ID secure scheme. Boldyreva*etal*.'s scheme still results in no.of problems: (1) Each user's private key size is 3log *n* points in an elliptic curve, where *n*is the number users in the binary tree. (2) The scheme also results in huge computation workload for encryption and decryption procedures. (3) It is huge load for Private Key Generator to maintain the binary tree with a large amount of users. Moreover, Seo and Emura [17] developed the security model of Boldyreva*et al*.'s revocable Identity-Based Encryption scheme [14] by considering a new threat, called decryption key exposure attacks. Based on the idea of Identity-Based Encryptionrt and Vergnaud's scheme [16], they also proposed a revocable Identity-Based Encryption scheme with decryption key exposure resistance. In order to decrease the sizes of both private keys and update keys, Park *et al*. [18] proposed a new revocable Identity-Based Encryption scheme by using multilinear maps,but the size of the public parameters is dependent to the number of users. For achieve constant the size of the public parameters, Wang *et al*. [19] employed both the double system encryption methodology [20] and the completes tree method [14] to propose a new revocable Identity-Based Encryption scheme. Moreover, Seo and Emura [21] extended the concept of revocable Identity-Based Encryption scheme to propose the first revocable Identity-Based Encryption scheme. In Seo and Emura's scheme, for each period, each user generates a secret key by multiplying some of the incomplete keys, which depends on the incomplete keys used by associates in the hierarchy tree. In that a case, the secret key size of each user increases quadratically 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. In 2015, Seo andEmura [22] proposed a new method to create a novelrevocable HIBE scheme with history-free updates. Nevertheless, the mention revocable Identity-Based Encryption and HIBE schemes above [17], [18], [19], [21], [22] employed the complete subtree method to decrease the number of key updates from linear to logarithmic in the number of users. However, these schemes also suffered from the same disadvantages ofBoldyreva*et al*.'s revocable Identity-Based Encryption scheme [14] and still used asecure channel to transmit periodic private keys.In 2012, Tseng and Tsai [23] proposed a new Revocable identity-Based Encryption scheme to remove the usage of secure channel between each user and the authority and use a public channel instead to transmit users' periodic private keys. They partition a user's private key into two components, namely, an identity key and a time update key. The identity key is a secret key associated with user's ID, which is sent to the user via a secure channel and remains fixed since being issued. The time update key is a key associated with user's ID and time period, which is changed along with time. The Private Key Generator periodically generates current time update keys for non-revoked users and sends them to these users via a public channel. A user is able to decrypt the cipher text if she/he possesses both the identitykey and the legitimate time update key. In other words, to revoke a particular user, the Private Key Generator simply stops issuing the new time update key for the user. However, the key-update efficiency is linear in theNumber of users so that the computation burden of Private Key Generator is still enormous. In 2015, by a cloud-aided service provider, Li *et al*. [24]introduced an outsourcing computation technique into Identity-Based Encryption to propose a revocable Identity-Based Encryption scheme with a key-update cloud service provider key-update cloud service provider They shifts the key-update procedures to a key-update cloud service provider to alleviate the load of Private Key Generator . Li *et al*. also used the similar technique adopted in Tseng and Tsai's scheme [23], which partitions a user's private key into an identity key and a time update key. The Private Key Generator sends a user the corresponding identity key via a secure channel. Meanwhile, the Private Key Generator must generate a random secret value (time key) for each user and send it to the key-update cloud service provider. Then the key-update cloud service provider generates the current time update key of a user by using the related time key and sends it to the user through a public channel. To revoke a user, the Private Key Generator just asks the key-update cloud service provider to stop issuing the new time update key of the user. Their system model is depicted in Fig. 1. However, their scheme has two shortcomings. First one is that the computation and communication costs are higher than previous revocable Identity-Based Encryption schemes [2], [23]. The Second shortcoming is unsociability in the sense that the key-update cloud service provider must keep a time key for each user so that it will incur the management load.

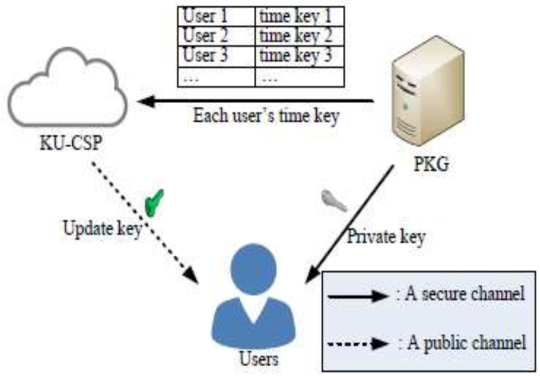


Fig. 1: Li *et al.*'s system model

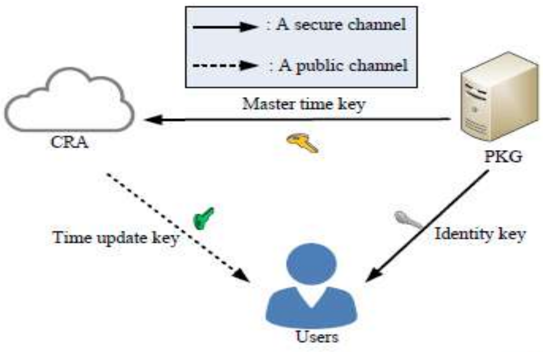


Fig. 2: System model for revocable IBE scheme with CRA

1.2 Our Contributions

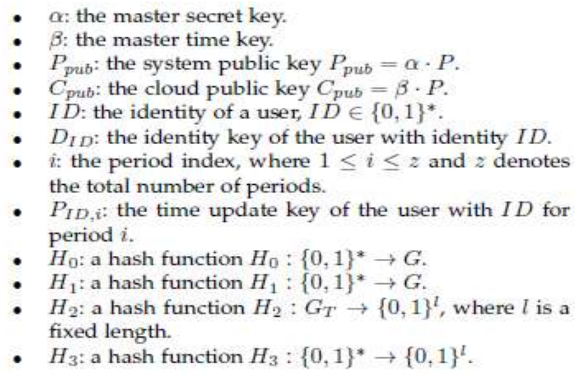
In order to solve both the un-scalability and the inefficiency in Li *et al*.'s scheme [24], we will propose a new revocable Identity-Based Encryption scheme with cloud revocation authority. The proposed scheme possesses the advantages of both Tseng and Tsai's revocable Identity-Based Encryption scheme [23] and Li *et al*.'s scheme [24]. In particular, each user's private key still consists of an identity key and a time update key. We introduce a cloud revocation authority to replace the role of the key-update cloud service provider in Li *et al*.'s scheme. The cloud revocation authority only needs to hold a random secret value (master time key) for all the users without affecting the security of revocable Identity-Based Encryption scheme. The cloud revocation authority 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 key-update cloud service provider. Our system model is depicted in Fig.2.

In this article, we first present the framework of our revocable Identity-Based Encryption scheme with Cloud Revocation Authority and define its security notions to model possible threats and attacks. Accordingly, a new revocable Identity-Based Encryption scheme with cloud revocation authority is proposed. As the adversary model presented in [23], [24], it consists of two adversaries, namely, an inside adversary (or a revoked user) and an outside adversary. For security analysis, we formally demonstrate that our scheme is semantically secure against adaptive-ID and chosen-cipher text attacks in the random oracle model under the bilinear decision Diffie-Hellman problem [2]. Finally, based on the proposed revocable Identity-Based Encryption scheme with Cloud Revocation Authority, we construct a cloud revocation authority aided authentication scheme with period-limited privileges for managing a large number of various cloud services. To demonstrate the merits of our scheme, Table 1 lists the comparisons among subtree-based Identity-Based Encryption schemes [14], [16], [17], [18], [19], HIBE schemes [21], [22], Tseng-Tsai scheme [23], Li *et al*.'s scheme [24] and ours in terms of the usage of key update channel, the size of each user's private key, key update load, outsourced computation of authority, the workload of the Private Key Generator and scalability of authority.

Those subtree-based Identity-Based Encryption schemes [14], [16], [17], [18], [19] and HIBE schemes [21], [22] employed the complete subtree method to decrease the number of 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. In Tseng and Tsai's revocable Identity-Based Encryption scheme [23], both the identity key and time update key are issued by the Private Key Generator . In order to alleviate the load of the Private Key Generator, Li *et al*. [24] employed a key update cloud service provider to share the responsibility of user revocation. In our revocable Identity-Based Encryption scheme, we employ a cloud revocation authority to perform user revocation. Indeed, the Private Key Generator in Li *et al*.'s scheme and ours may also perform the revocation operations. Both the key-update cloud service provider and the cloud revocation authority are designated to share responsibility for performing user revocation. For scalability, the key-update cloud service provider in Li *et al*.'s scheme must keep *n* various time keys for *n* users so that it does not possess scalability and incurs the management load. On the contrast, the Cloud Revocation Authority in our scheme holds only one master time key for all the users. When the number *n* of users in the system is very large, the Private Key Generator may designate multiple Cloud Revocation Authority s to share the responsibility of user revocation while each Cloud Revocation Authority holds only the same master time key. However, in Li et al.'s scheme, each key-update cloud service provider must also keep *n* time keys. Indeed, cloud computing is a ubiquitous computing environment so that putting multiple Cloud Revocation Authority s on clouds may provide convenient management of user revocation while reducing the load of the single Private Key Generator. The detailed comparisons regarding computation and communication efficiency will be given in Section 6.

2.System Operations And Security

For convenience, we first define the following notations.



- α: the master secret key.
- β: the master time key.
- P_{pub}: the system public key $P_{pub} = \alpha \cdot P$.
- C_{pub}: the cloud public key $C_{pub} = \beta \cdot P$.
- ID: the identity of a user, $ID \in \{0,1\}^*$.
- D_{ID}: the identity key of the user with identity ID.
- i: the period index, where $1 \leq i \leq z$ and z denotes the total number of periods.
- $P_{ID,i}$: the time update key of the user with ID for period i.
- H_0: a hash function $H_0 : \{0,1\}^* \to G$.
- H_1: a hash function $H_1 : \{0,1\}^* \to G$.
- H_2: a hash function $H_2 : G_T \to \{0,1\}^l$, where l is a fixed length.
- H_3: a hash function $H_3 : \{0,1\}^* \to \{0,1\}^l$.

2.1 System Operations

In Fig. 3, we present the system operations of the proposed revocable Identity-Based Encryption scheme with Cloud Revocation Authority . Our system has three roles, namely, a private key generator , a cloud revocation authority and users (senders and receivers). First, the Private Key Generator selects a master secret key *α* a master time key*β* and a total number *z* of periods, and sends the master time key *β*to the Cloud Revocation Authority . The Private Key Generator uses the master secret key _ to compute the identity key $D_{ID}$of the user with identity *ID*, and sends the identity key $D_{ID}$to the user via a secure channel. On the other hand, the Cloud Revocation Authority is responsible to produce the time update keys for all the non-revoked users by using the master time key *α*. To do this, at the starting of each period *i*, the Cloud Revocation Authority uses the master time key _ and a non-revoked user's identity *ID* to generate the current time update key $P_{ID,i,}$and sends it to the user via a public channel (e.g. e-mail). When a sender wants to transmit a message *M* to a receiver with identity *ID* at period *i*, the sender produces a cipher text$C = E_{(ID,i,M)}$and sends it to the receiver, where *E* denotes the encryption algorithm of our revocable Identity-Based Encryption scheme with Cloud Revocation Authority . Upon receiving the cipher text, the receiver uses the identity key $D_{ID}$and time update key P_{ID}ito decrypt the cipher text.

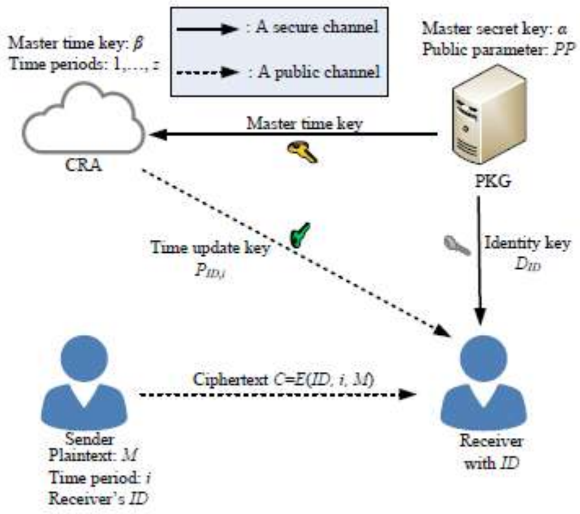


Fig. 3: System operations of revocable IBE scheme with CRA

2.2 Framework

In this section, we present the syntax of revocable Identity-Based Encryption schemes with Cloud Revocation Authority .

Definition 1.A revocable Identity-Based Encryption scheme with Cloud Revocation Authority consists of five algorithms: *system setup*, *identity key extract*, *time keyupdate*, *encryption* and *decryption*.

- *System setup* is a probabilistic algorithm that is run by the Private Key Generator . The Private Key Generator takes as input two parameters, namely, a secure parameter $\lambda$and the total number z of periods, and outputs public parameters *PP*, a master secret key α and a master time key β. Finally, it sends β. to the Cloud Revocation Authority via a secure channel. *PP* are made public to all the following algorithms.
- Identity key extract is a deterministic algorithm which is run by the Private Key Generator that takes as input the master secret key α and a user's identity *ID*, and outputs the corresponding identity key D_{ID}. Then, the Private Key Generator returns $D_{ID}$to the user via a secure channel.
- *Time key update* is a deterministic algorithm which is run by the Cloud Revocation Authority. The Cloud Revocation Authority uses the master time keyβ, a user's identity *ID* and a period *i* to compute theuser's time update key $P_{ID,I}$ for period *i*. Then, the Cloud Revocation Authority returns the time update key $P_{ID,i}$to the user via a public channel (e.g. e-mail or public board).
- *Encryption* is probabilistic algorithm that is run by auser (sender). The sender takes as input a message*M*, a receiver's identity *ID* and a current period *i*,and outputs a cipher text *C*.
- *Decryption* is a deterministic algorithm which is runby a user (receiver). The receiver takes as input aciphertext *C* and the private key pair (D_{ID}, $P_{ID,i)}$,and outputs the corresponding plaintext *M*.

3.Cloud Computing Applications

In this section, we extend our revocable Identity-Based Encryption scheme to discuss two extended cloud computing applications, namely, the revocable attribute-based encryption for cloud storage and the Cloud Revocation Authority-aided authentication with period-limited privileges for managing a large number of various cloud services.

3.1 Revocable attribute-based encryption

With the rapid development in wireless communication, cloud storage services [34] have become popular increasingly. Users can store their data on the cloud storage so that they may access their data anywhere at any time. Typically, the data stored on the cloud storage is encrypted for user privacy while protecting from access by other users. Indeed, due to the collaborative property of some applications, a data owner allows specific parties to decrypt the encrypted data stored on the cloud storage. In such a situation, enforcingthis kind of access control by ordinary public key encryption (ex. Identity-Based Encryption) schemes is not very convenient because it cannot provide the flexibility of users to share their data. Attribute-based encryption [35] is regarded as one of the most suitable encryption schemes for data sharing of cloud storage. Indeed, Attribute-based encryption is encryption for privileges, not for users so that an Attribute-based encryption scheme is a very useful tool for cloud storage services since data sharing is an important feature for such services.

In 2005, Sahai and Waters [35] first introduced the concept of attribute-based encryption which refines Identity-Based Encryption scheme [2] by associating cipher texts and a set of attributes. In an Attribute-based encryption scheme, the Private Key Generator typically sends the corresponding attribute keys for the user with several attributes. An Attribute-based encryption scheme allows a data owner to encrypt data under a set of attributes associated with access structures, and users who own these corresponding attribute keys are able to decrypt the encrypted data. Afterward, there are numerous Attribute-based encryption schemes [36], [37], [38], [39] that have been proposed. Indeed, we may combine the revocability concept of the proposed revocable Identity-Based Encryption scheme with the existing Attribute-based encryption schemes to construct revocable Attribute-based encryption schemes. Indeed, Li *et al*. [40] and Qian*et al*. [41], respectively, proposed an Attribute-based encryption scheme with user/attribute revocation for various applications. Both schemes still adopt the sub-tree method in [14] to address the revocation rekeying issue so that a secure channel is used to transmit the new updated user keys and attribute keys.For constructing such revocable Attribute-based encryption schemes using a public channel, we may employ the same role of the Cloud Revocation Authority to be responsible for periodically generating the attribute-time keys for users and send them to users via a public channel. The functionality of the attribute-time key is the same with that of the time update key in the proposed revocable Identity-Based Encryption scheme. Therefore, if a data owner encrypts data under a set of attributes associated with access structures and a time period. Thus, users who own both the attribute keys and valid attribute-time keys at the time period are able to decrypt the encrypted data. If a particular attribute of a user is revoked, the Cloud Revocation Authority simply stops issuing the new corresponding attribute-time key for the user. Therefore, arevocable Attribute-based encryption scheme provides more flexible than an Attribute-based encryption scheme for managing attributes of users.

3.2Cloud Revocation Authority -Aided Authentication Scheme With Period Limited Privileges

An authentication scheme is a cryptographic mechanism to authenticate users over public networks. Before a user gains access to a server's services, the user must be authenticated and authorized by the server. Here, we extend our revocable Identity-Based Encryption scheme to construct a cloud revocation authority(Cloud Revocation Authority) aided authentication scheme with period limited privileges for managing a large number of various cloud services [34]. When a company (or organization) constructs numerous various cloud services, how to efficiently manage the authorizations for these cloud services is an important issue since a user must authenticate herself/ himself to a cloud service server before accessing the cloud services. In the system with multiple cloud services, multiple Cloud Revocation Authority s replace the role of The Cloud Revocation Authority in our proposed scheme. The master time key is replaced with multiple master privilege keys. A Cloud Revocation Authority with a master privilege key can manage the corresponding privilege to have access to some service server at various periods. A Cloud Revocation Authority is able to use its master privilege key to generate and send a period-limited privilege key to a user. A user with both the associated identity key and a period-limited privilege key is able to access the corresponding server. Indeed, a Cloud Revocation Authority may also manage single or multiple service servers. Without loss of generality, we assume that there are *k* independent Cloud Revocation Authority that are responsible for managing *k* independent service servers, respectively.

For simplicity, we illustrate the case *k* = 2 by Fig. 4. The private key generator randomly selects *k* different master privilege keys β_1,β_2....$\beta_k$and sends each $\beta_j$to the corresponding Cloud Revocation Authority*j*, respectively. Also, the Private Key Generator sends the identity key $D_{ID}$to a legitimate user with identity *ID* via a secure channel. On the

other hand, if this user with identity *ID* is granted to have access to the service server *j* at period *i*, the Cloud Revocation Authorityj will use the master privilege key βj to generate the period-limited privilege key $P_{IDi,j}$and send it to the user via a public channel. Consequently, the user is able to access the server *j* at period *i* by using both the identity key $D_{ID}$and periodlimited privilege key $P_{IDi,j}$Note that, indeed, a Cloud Revocation Authority may manage all the privileges for all the service servers. In such a case, all the master privilege keys are sent to the designated Cloud Revocation Authority .

In the system with multiple cloud services, a user with both the identity key D_{ID} and period-limited privilege key $P_{IDi,j}$may run an authentication scheme, ca$P_{IDi,j}$ Cloud Revocation Authority aided authentication scheme with period-limited privileges,to authenticate herself/himself to the service server *j* at period *i*. The proposed Cloud Revocation Authority-aided authentication scheme with period-limited privileges depicted in Fig. 5, which consists of four algorithms :

System setup: As in the revocable Identity-Based Encryption scheme with Cloud Revocation Authority proposed in Section 3, a trusted Private Key Generator generates the master secret key $\alpha$and computes the system public key $P_{pub}= \alpha.P$. In addition, suppose thatthere are *k* independent service servers managed by *k*independent Cloud Revocation Authoritys in the system. The Private Key Generator randomly selects *k* different master privilege

keys $\beta 1; \beta 2 \ldots\ldots \beta k$ and sends each βj to the correspondingCloud Revocation Authority*j*via a secure channel, respectively. In themeantime, the Private Key Generator also computes the privilegepublickey$C_{pub,j}= \beta j\ .P$ for each Cloud Revocation Authority *j*.

In the following, based on the IND-ID-CCA security of the revocable Identity-Based

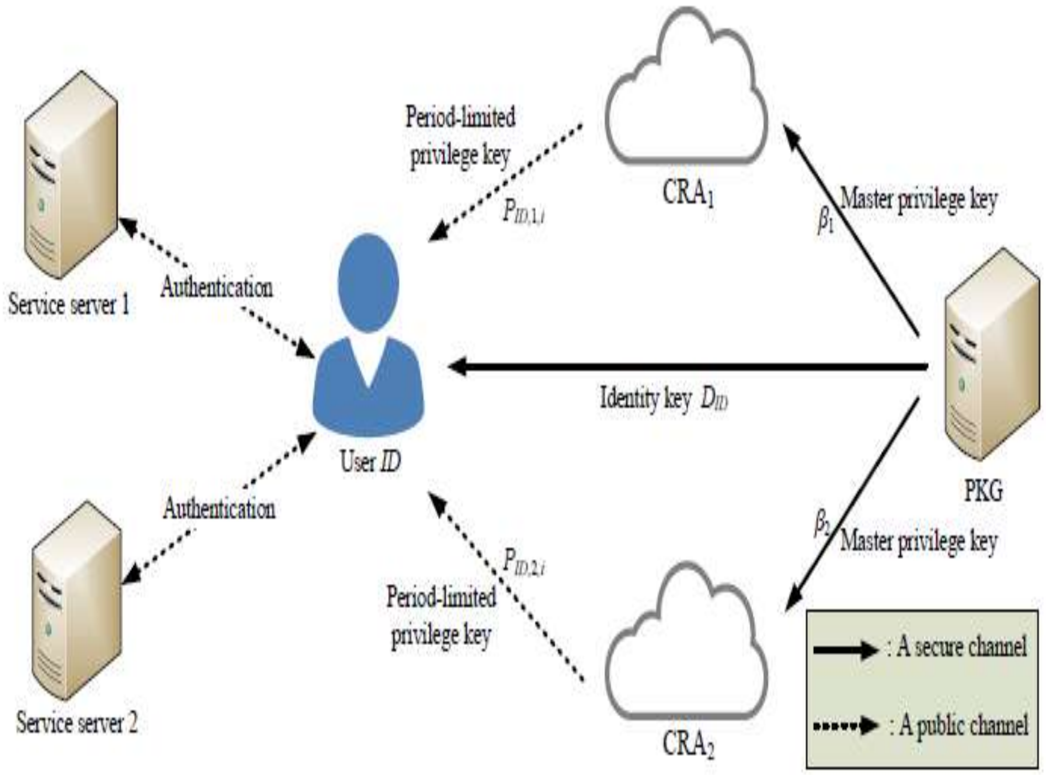


Fig. 4: Example of system model for managing multiple cloud services

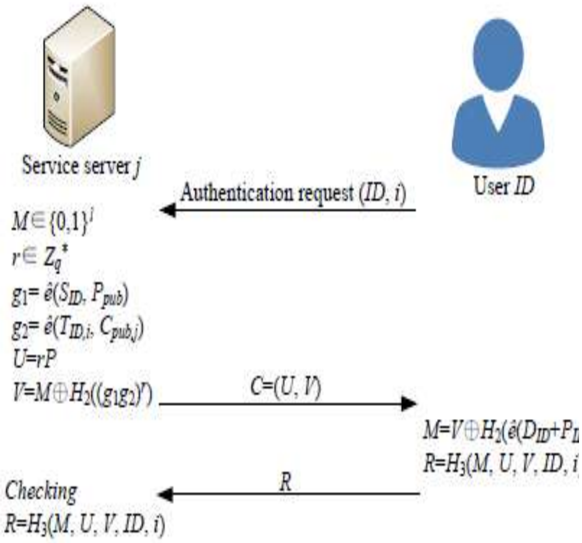

Service server j
User ID
Authentication request (ID, i)
$M\in\{0,1\}^l$
$r\in Z_q^*$
$g_1=\hat{e}(S_{ID}, P_{pub})$
$g_2=\hat{e}(T_{ID,i}, C_{pub,j})$
$U=rP$
$V=M\oplus H_2((g_1g_2)^r)$
$C=(U, V)$
$M=V\oplus H_2(\hat{e}(D_{ID}+P_{I}$
$R=H_3(M, U, V, ID, i$
R
Checking
$R=H_3(M, U, V, ID, i)$

Fig. 5: Authentication procedure

the proposed Cloud Revocation Authority -aided authentication scheme with periodlimited privileges is secure under active attacks.

4. Conclusion

In this article, I proposed a new revocable Identity-Based Encryption scheme with a cloud revocation authority , in which the revocation procedure is performed by the Cloud Revocation Authority to improve the load of the Private Key Generator. This outsourcing computation technique with other authorities has been employed in Li *et al.*'s revocable Identity-Based Encryption scheme with Key Update – Cloud Service Provider. However, this scheme requires higher computational and communicational costs than earlier proposed Identity-Based Encryption schemes. For the time key update procedure, the Key Update -Cloud Service Provider in Li *et al.*'s scheme should keep a secret value for each user so that it is need of scalability. In revocable Identity-

Based Encryption scheme With Cloud Revocation Authority, the Cloud Revocation Authority 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. For security analysis, we have demonstrated that our scheme is semantically secure against adaptive-ID attacks under the decisional bilinear Diffie-Hellman assumption. Finally, based on the proposed revocable Identity-Based Encryption scheme with Cloud Revocation Authority , we constructed a Cloud Revocation Authority aided authentication scheme with period-limited privileges for managing a large number of various cloud services.

5. 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.

[8] V. Goyal, "Certificate revocation using fine grained certificate space partitioning," Proc. Financial Cryptography, LNCS, vol. 4886, pp. 247-259, 2007.

[9] D. Boneh, X. Ding, G. Tsudik, and C.-M. Wong, "A Method for fast revocation of public key certificates and security capabilities," Proc.10th USENIX Security Symp., pp. 297-310. 2001.

[10]X. Ding and G. Tsudik, "Simple identity-based cryptography with mediated RSA," Proc. CT-RSA'03, LNCS, vol. 2612, pp. 193-210,2003.

[11] B. Libert and J. J. Quisquater, "Efficient revocation and threshold pairing based cryptosystems," Proc. PODC2003, pp. 163-171, 2003.

[12] J. Baek and Y. Zheng, "Identity-based threshold decryption," Proc. PKC'04, LNCS, vol. 2947, pp. 262-276, 2004.

[13] H.-S. Ju, D.-Y. Kim, D.-H. Lee, H. Park, and K. Chun, "Modified ID-based threshold decryption and its application to mediated IDbased encryption," Proc. APWeb2006, LNCS, vol. 3841, pp. 720-725, 2006.

[14]A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with efficient revocation," Proc. CCS'08, pp. 417-426, 2008.

[15]A. Sahai and B. Waters, "Fuzzy identity-based encryption," Proc. Eurocrypt'05, LNCS, vol. 3494, pp. 557-557, 2005.

[16]B. Libert and D. Vergnaud, "Adaptive-ID secure revocable identity-based encryption," Proc. CT-RSA'09, LNCS, vol. 5473, pp.1-15, 2009.

[17]J.-H. Seo and K. Emura, "Revocable identity-based encryption revisited: security model and construction," Proc. PKC'13, LNCS,vol. 7778, pp. 216-234, 2013.

[18]S. Park, K. Lee, and D.H. Lee, "New constructions of revocable identity-based encryption from multilinear maps," IEEE Transactions on Information Forensics and Security, vol.10 , no. 8, pp. 1564 - 1577, 2015.

[19]C. Wang, Y. Li, X. Xia, and K. Zheng, "An efficient and provable secure revocable identity-based encryption scheme," PLoS ONE, vol. 9, no. 9, article: e106925, 2014.

[20]A. Lewko A and B. Waters, "New techniques for dual system encryption and fully secure hibe with short ciphertexts," Proc.TCC'10, LNCS, vol. 5978, pp. 455-479, 2010.

[21]J.-H. Seo and K. Emura, "Efficient delegation of key generation and revocation functionalities in identity-based encryption," Proc. CT-RSA'13, LNCS, vol. 7779, pp. 343-358, 2013.

[22]J.-H. Seo and K. Emura, "Revocable hierarchical identity-based encryption: history-free update, security against insiders, and short Ciphertexts," Proc. CT-RSA'15, LNCS, vol. 9048, pp. 106-123, 2015.

[23]Y.-M. Tseng. and T.-T. Tsai, "Efficient revocable ID-based encryption with a public channel," Computer Journal, vol.55, no.4, pp. 475-486, 2012.

[24]J. Li, J. Li, X. Chen, C. Jia, and W. Lou, "Identity-based encryption with outsourced revocation in cloud computing," IEEE Trans. On Computers, vol. 64, no. 2, pp. 425-437, 2015.

[25]S. Galbraith, K. Paterson, and N. P. Smart, "Pairings for cryptographers," Discrete Applied Mathematics, vol. 156, no. 16, pp. 3113- 3121, 2008.

[26]E. Fujisaki and T. Okamoto, "How to enhance the security of public-key encryption at minimum Cost," Proc. PKC'99, LNCS, vol. 1560, pp. 53-68, 1999.

[27]T. Kitagawa, P. Yang, G. Hanaoka, R. Zhang, K. Matsuura, and H. Imai, "Generic transforms to acquire CCA-security for identity based encryption: The Cases of FOPKC and REACT," Proc. ACISP'06, LNCS, vol. 4058, pp. 348-359, 2006.

[28]J. S. Coron, "On the exact security of full domain hash," Proc. Crypto'00, LNCS, vol. 1880, pp. 229-235, 2000.

[29]M. Scott, "Computing the Tate pairing," Proc. CT-RSA'05, LNCS, vol. 3376, pp. 293-304, 2005.

[30]M. Scott, N. Costigan, and W. Abdulwahab, "Implementing cryptographic pairings on smartcards," Proc. CHES'06, LNCS, vol. 4249, pp. 134-147, 2006.

[31]T.-Y. Wu and Y.-M. Tseng, "An efficient user authentication and key exchange protocol for mobile client-server environment," Computer Networks, vol. 54, no. 9, pp. 1520-1530, 2010.

[32]B. Lynn (2015), Java Pairing Based Cryptography Library (JPBC) [Online]. Available: http://gas.dia.unisa.it/projects/jpbc/benchmark.html

[33]A. Wander, N. Gura, H. Eberle, V. Gupta, and S. Shantz, "Energy analysis of public-key cryptography for wireless sensor networks," Proc. 3rd IEEE International Conf. Pervasive Computing Commun, pp. 324-328, 2005.

[34]M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A view of cloud computing," Commun. ACM, vol. 53, no. 4, pp. 50-58, 2010.

[35]A. Sahai and B. Waters, "Fuzzy identity-based encryption," Proc. Eurocrypt'05, LNCS, vol. 3493, pp. 457-473, 2005.

[36]V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," Proc. ACM CCS, pp. 89-98, 2006.

[37]A. Sahai, H. Seyalioglu, and B. Waters, "Dynamic credentials and ciphertext delegation for attribute-based encryption," Proc.Crypto'12, LNCS, vol. 7417 , pp. 199-217, 2012.

[38]S. Hohenberger and B. Waters, "Attribute-based encryption with fast decryption," Proc. PKC'13, LNCS, vol. 7778, pp. 162-179, 2013.

[39]P.-W. Chi and C.-L. Lei, "Audit-free cloud Storage via deniable attribute-based encryption," IEEE Transactions on Cloud Computing, article in press (DOI: 10.1109/TCC.2015.2424882), 2015.

[40]J. Li, Y. Shi, and Y. Zhang, "Searchable ciphertext-policy attributebased encryption with revocation in cloud storage," International Journal of Communication Systems, article in press (DOI: 10.1002/dac.2942), 2015.

[41]H. Qian, J. Li, Y. Zhang, and J. Han, "Privacy preserving personal health record using multi-authority attribute-based encryption with revocation," International Journal of Information Security, vol. 14, no. 6, pp. 487-497, 2015.

[42]A. Fiat and A. Shamir, "How to prove yourself: practical solutions to identification and signature Problems," Proc. Crypto' 86, LNCS, vol. 263, pp. 186-194, 1987.

[43]K. Kurosawa and S. Heng, "From digital signature to ID-based identification/signature," Proc. PKC'04, LNCS, vol. 2947, pp 248- 261, 2004.

[44]M. Feldhofer, S. Dominikus, and J. Wolkerstorfer, "Strong authentication for RFID systems using the AES algorithm," Proc. CHES'04,LNCS, vol. 3156, pp. 357-370, 2004.

[45]Y.-M. Tseng, T.-Y. Wu, and J.-D. Wu, "A pairing-based user authentication scheme for wireless clients with smart cards,"

Informatica,
vol. 19, no. 2, pp. 285-302, 2008.

[46]*C. Kaufman, P. Hoffman, Y. Nir, P. Eronen, and T. Kivinen, "Internet key exchange protocol version 2 (IKEv2) ," IETF, RFC 7296,2014.*

[47] *A. Freier, P. Karlton, and P. Kocher, "The secure sockets layer (SSL) protocol version 3.0," IETF, RFC 6101, 2011*

Author's Profile:

Madasu Surekha, PG Scholar, Dept of CSE, Pace Institute of Technology & Sciences, Ongole, A.P

D.Anandam, Assistant Professor, Dept of CSE, Dept of CSE, PACE Institute of Technology & Sciences, Ongole, A.P, India. He Have 10 Years of Teaching Experience.