ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 21, August 2017

Authentic Data Sharing by Using Revocable-Storage Identity-Based Encryption in cloud computing

Mrs.M.durgadevi,Msc,MCA,Mtech(CSE)[1], Mrs.M.Naga pavani,Msc[2]
[1,2]Lecturer in Mathematics, **CH.S.D.ST Theresa's College for Women,Eluru, India.**
m.devi.mca.06@gmail.com[1]
pavanivenkat0143@gmail.com[2]

Abstract—Cloud computing provides a flexible and convenient way for data sharing, which brings various benefits for both thesocietyand individuals. But there exists a natural resistance for users to directly outsource the shared data to the cloud server since the dataoften contain valuable information. Thus, it is necessary to place cryptographically enhanced access control on the shared data.Identity-based encryption is a promising cryptographical primitive to build a practical data sharing system. However, access control isnot static. That is, when some user's authorization is expired, there should be a mechanism that can remove him/her from thesystem.
Consequently, the revoked user cannot access both the previously and subsequently shared data. To this end, we propose a notioncalled revocable-storage identity-based encryption (RS-IBE), which can provide the forward/backward security of ciphertext byintroducing the functionalities of user revocation and ciphertext update simultaneously. Furthermore, we present a concrete construction of RS-IBE, and prove its security in the defined security model. The performance comparisons indicate that the proposedRS-IBE scheme has advantages in terms of functionality and efficiency, and thus is feasible for a practical and cost-effectivedata-sharing system. Finally, we provide implementation results of the proposed scheme to demonstrate its practicability.

Key words—Cloud computing, data sharing, revocation, Identity-based encryption, ciphertext update, decryption key exposure.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 21, August 2017

I.Introduction

CLOUD computing is a paradigm that provides massive computation capacity and huge memory space at a low cost. It enables users to get intended services irrespective of time and location across multiple platforms (e.g., mobile devices, personal computers), and thus brings great convenience to cloud users. Among numerous services provided by cloud computing, cloud storage service, such as Apple's I Cloud, Microsoft's Azureand Amazon's S3 , can offer a more flexible and easy way to share data over the Internet, which provides various benefits for our society . However, it also suffers from several security threats, which are the primary concerns of cloud users .Firstly, outsourcing data to cloud server implies that data is out control of users. This may cause users' hesitation since the outsourced data usually contain valuable and sensitive information. Secondly, data sharing is often implemented in an open and hostile environment, and cloud server would become a target of attacks. Even worse, cloud server itself may reveal users' data for illegal profit. Thirdly, data sharing is not static. That is, when a user's authorization gets expired, he/she should no longer possess the privilege of accessing the previously and subsequently shared data. Therefore, while outsourcing data to cloud server, users also want to control access to these data such that only those currently authorized users can share the outsourced data.

A kind of identity-based access control placed on the shared data should meet the following security goals:

• **Data confidentiality**: Unauthorized users should beprevented from accessing the plaintext of the shareddata stored in the cloud server. In addition, the cloudserver, which is supposed to be honest but curious, should also be deterred from knowing plaintext ofthe shared data.

• **Backward secrecy**: Backward secrecy means that,when a user's authorization is expired, or a user'ssecret key is compromised, he/she should be preventedfrom accessing the plaintext of the *subsequently*shared data that are still encrypted under his/heridentity.

• **Forward secrecy**: Forward secrecy means that, whena user's authority is expired, or a user's secret keyis compromised, he/she should be prevented fromaccessing the

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 21, August 2017

plaintext of the shared data that can be*previously* accessed by him/her.

The specific problem addressed in this paper is how to construct a fundamental identity-based cryptographical tool to achieve the above security goals.

II.Motivation

It seems that the concept of revocable identity-based encryption (RIBE) might be a promising approach that fulfills
the aforementioned security requirements for data sharing. RIBE features a mechanism that enables a sender to append the current time period to the ciphertext such that the receiver can decrypt the ciphertext only under the condition that he/she is not revoked at that time period. RIBE-based data sharing system works as follows:

Step 1: The data provider (e.g., David) first decides the users (e.g., Alice and Bob) who can share the data.

Then, David encrypts the data under the identities Alice and Bob, and uploads the cipher text of the shared data to the cloud server.

Step 2: When either Alice or Bob wants to get the shared data, she or he can download and decrypt the corresponding cipher text. However, for an unauthorized user and the cloud server, the plaintext of the shared
data is not available.

Step 3: In some cases, e.g., Alice's authorization gets expired, David can download the cipher text of the shared data, and then decrypt-then-re-encrypt the shared data such that Alice is prevented from accessing the plaintext of the shared data, and then upload the re-encrypted data to the cloud server again.

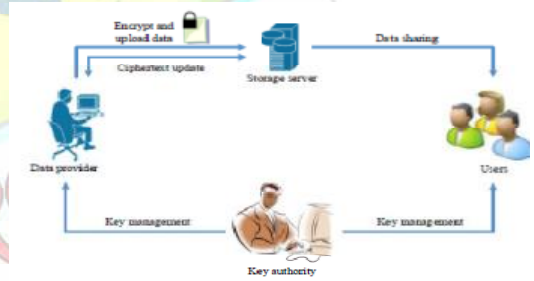

Fig. 1. A natural RIBE-based data sharing system

Obviously, such a data sharing system can provide confidentiality and backward secrecy. Furthermore, the method of decrypting and re-encrypting all the shared data can ensure forward secrecy. However, this brings new challenges. Note that the

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 21, August 2017

process of decrypt-then-re-encrypt necessarily involves users' secret key information, which makes the overall data sharing system vulnerable to new attacks. In general, the use of secret key should be limited to only usual decryption, and it is inadvisable to update the cipher text periodically by using secret key.

Another challenge comes from efficiency. To update the cipher text of the shared data, the data provider has to frequently carry out the procedure of download-decrypt-re encrypt- upload. One method to avoid this problem is to require the cloud server to directly re-encrypt the cipher text of the shared data. In addition, the technique of proxy re-encryption can also be used to conquer the aforementioned problem of efficiency. Unfortunately, it also requires users to interact with the cloud server in order to update the cipher text of the shared data.

- **Related work**
  - ***Revocable identity-based encryption***

The concept of identity-based encryption was introduced by Shamir , and conveniently instantiated by Boneh and Franklin . IBE eliminates the need for providing a public key infrastructure (PKI). Regardless of the setting of IBE or PKI, there must be an approach to revoke users from the system when necessary, e.g., the authority of some user is expired or the secret key of some user is disclosed.

Boneh and Franklin first proposed a natural revocation way for IBE. They appended the current time period to the cipher text, and non-revoked users periodically received private keys for each time period from the key authority. Unfortunately, such a solution is not scalable, since it requires the key authority to perform linear work in the number of non-revoked users. In addition, a secure channel is essential for the key authority and non-revoked users to transmit new keys. [7] proposed a secure hash message authentication code. A secure hash message authentication code to avoid certificate revocation list checking is proposed for vehicular ad hoc networks (VANETs). The group signature scheme is widely used in VANETs for secure communication, the existing systems based on group signature scheme provides verification delay in certificate revocation list checking. In order to overcome this delay

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 21, August 2017

this paper uses a Hash message authentication code (HMAC). It is used to avoid time consuming CRL checking and it also ensures the integrity of messages. The Hash message authentication code and digital signature algorithm are used to make it more secure . In this scheme the group private keys are distributed by the roadside units (RSUs) and it also manages the vehicles in a localized manner. Finally, cooperative message authentication is used among entities, in which each vehicle only needs to verify a small number of messages, thus greatly alleviating the authentication burden.

- ***Forward-secure cryptosystems***

  In 1997, Anderson introduced the notion of forward security in the setting of signature to limit the damage of

key exposure. The core idea is dividing the whole lifetime of a private key into T discrete time periods, such that
the compromise of the private key for current time period cannot enable an adversary to produce valid signatures for previous time periods. Subsequently, Bellare and Miner provided formal definitions of forward-secure signature and presented practical solutions. Since then, a large number of forward-secure signature schemes has been proposed.

III. Bilinear pairing and complexity assumption

Definition 1 (**Bilinear pairing**). *Let* G_1 *and* G_2 *be two cyclic groups with prime order* q, *and* g *be a generator of* G_1. *A bilinear pairing is a map* $e : G_1 \times G_1 \rightarrow G_2$ *with the following properties:*

Bilinearity: $e(u^a, h^b) = e(u, h)^{ab}$ *for all* $u, h \in G_1$, $a, b \in Z_q^*$.

Non-degeneracy: $e(g, g) \neq 1$.

Computability: There exists an efficient algorithm to compute $e(u, h)$ *for any* $u, h \in G_1$.

Definition 2 (**Decisional ℓ-BDHE Assumption**).*The decisional ℓ-BDHE problem is formalized as follows. Choose a group* G_1 *with prime order* p *according to the security parameter* λ. *Select a generator* g *of* G_1 *and* $a, s \leftarrow R Z_p$, *and let* $f_i = g^{a^i}$ *Provide the vector* $\boldsymbol{f} = (g, g^s, f_1, ..., f_\ell, f_{\ell+2}, ..., f_{2\ell})$ *and an element* $D \in G_2$ *to a probabilistic polynomial-time (PPT) algorithm* C, *it outputs 0 to indicate that* $D = e(g^s, g^{a^{\ell+1}})$, *and outputs 1 to indicate that* D *is a random element from* G_2.*The advantage of* C *solving the decisional ℓ-BDHE problem in* G_1 *is defined as follows:*

$\mathbf{Adv}^{\ell-dBDHEC}(\lambda) = \left| \Pr[C(\boldsymbol{f}, D = e(g^s, g^{a^{\ell+1}})) = 0] - \Pr[C(\boldsymbol{f}, D \leftarrow RG_2) = 0] \right|$

We say that the decisional ℓ-BDHE assumption holds in G1 *provided that no PPT algorithm can solve the decisional ℓ-*

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 21, August 2017

BDHEproblem with a non-negligible advantage.

KUNodes algorithm

Our RS-IBE scheme uses the same binary tree structure introduced by Boldyreva, Goyal and Kumar to achieve efficient revocation. To describe the revocation mechanism, we first present several notations. Denote by ε the root node of the binary tree BT , and Path(η) the set of nodes on the path from ε to the leaf node η (including ε and η). For a non-leaf node θ, we let θland θrstand for its left and right child, respectively. Given a time period t and revocations list RL, which is comprised of the tuples (ηi, ti) indicating that the node ηiwas revoked at time period ti, the algorithm KUNodes(BT ,RL, t) outputs the smallest subset Y of nodes of BT such that Y contains an ancestor for each node that is not revoked before the time period t.

Informally, to identify the set Y, the algorithm first marks all the ancestors of revoked nodes as revoked, then outputs all the non-revoked children of revoked nodes.

Algorithm 1 KUNodes(BT ,RL, t)
1: X,Y←–∅
2: **for all** (ηi, ti) ∈RL **do**
3: **if** ti≤t **then**
4: Add Path(ηi) to X
5: **end if**
6: **end for**
7: **for all** θ∈X **do**
8: **if** θl/∈X **then**
9: Add θlto Y
10: **end if**
11: **if** θr/∈X **then**
12: Add θrto Y
13: **end if**
14: **end for**
15: **if** Y = ∅ **then**
16: Add the root node εto Y
17: **end if**
18: **return** Y.

- **Syntax of RS-IBE**

Definition (Revocable-Storage Identity-Based Encryption).

A revocable-storage identity-based encryption scheme with message space M, *identity space* I *and total number of time periods* T *is comprised of the following seven polynomial time algorithms:*

- **Setup**(1λ, T,N)*: The setup algorithm takes as input the security parameter* λ, *the time bound* T *and the maximum number of system users* N, *and it outputs the public parameter* PP *and the master secret key* MSK, *associated*

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 21, August 2017

with the initial revocation list RL = □ *and state* st.

- **PKGen**(PP,MSK, ID)*: The private key generation algorithm takes as input* PP, MSK *and an identity* ID ∈ I*, and it generates a private key* SKID *for* ID *and an updated state* st.
- **KeyUpdate**(PP,MSK,RL, t, st)*: The key update algorithm takes as input* PP,MSK*, the current revocation list* RL*, the key update time* t ≤ T *and the state* st*, it outputs the key update* KUt.
- **DKGen**(PP, SKID,KUt)*: The decryption key generation algorithm takes as input* PP, SKID *and* KUt*, and it generates a decryption key* DKID,t*for* ID *with time period* t *or a symbol* ⊥ *to illustrate that* ID *has been previously revoked.*
- **Encrypt**(PP, ID, t,M)*: The encryption algorithm takes as input* PP*, an identity* ID*, a time period* t ≤ T *,and a message* M ∈ M *to be encrypted, and outputs a cipher text* CTID,t.
- **CTUpdate**(PP,CTID,t, t′)*: The ciphertext update algorithm takes as input* PP, CTID,t*and a new time period* t′ ≥ t*, and it outputs an updated ciphertext* CTID,t′ .
- **Decrypt**(PP, CTID,t,DKID,t′)*: The decryption algorithm takes as input* PP, CTID,t, DKID,t′ *, and it recovers the encrypted message* M *or a distinguished symbol* ⊥ *indicating that* CTID,t*is an invalid ciphertext.*
- **Revoke**(PP, ID,RL, t, st)*: The revocation algorithm takes as input* PP*, an identity* ID ∈ I *to be revoked, the current revocation list* RL*, a state* st*and revocation time period* t ≤ T *, and it updates* RL *to a new one.*

Our construction involves two binary trees BT and T to manage identity and time period, respectively. Moreprecisely, for identity revocation, we follow Boldyreva etal.'s strategy. That is, given an identity ID, we randomlystore it in a leaf node η of BT , and generate thecorresponding secret key SKID = {(θ, SKID,θ)}θ∈Path(η)as in previous RIBE schemes . If the user IDis not

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 21, August 2017

revoked at time period t, there exists a node $\theta \in Path(\eta) \cap KUNodes(BT, RL, t)$. Consequently, given theupdate key $KUt=\{(\theta,KUt,\theta)\}\theta \in KUNodes(BT, RL,t)$, the userID can obtain the decryption key for time period t byre-randomizing and combining $(\theta, SKID,\theta)$ and (θ,KUt,θ). However, for a user that is revoked at time period t, there is no such node. As a result, the user cannot decrypt the ciphertext that is produced under its identity after the time period t (including t).

Let $T = 2\ell$ be the total number of system time periods. For each $1 \leq i \leq T$, the time period $ti \in \{0, 1\}\ell$ is associated with the i-th leaf node vtiof T . Here, we arrange all leaf nodes of T in numerical order from left to right. Given a node v of T , let $bv \in \{0, 1\}\leq\ell$ be the binary sequence corresponding to the path from the root node of T to v, where 0 and 1 indicate that the path passes through the left and right child of the parent node, respectively. Conversely, given a string $b \in \{0, 1\}\leq\ell$, let vbbe the node that has a path b from the root node to it. Furthermore, denote by bv[j] and ti[j] the j-th bit of bvand tirespectively, and |bv| the length of bv.

IV.Security analysis

Theorem 1.*If there exists a PPT adversary* A *breaking the INDRID-CPA security of the proposed RS-IBE scheme, then there exists an algorithm* C *solving the decisional* ℓ*-BDHE problem such that*
Advℓ−dBDHEC(λ) ≥1/ 32T q2(n + 1)**Adv**IND-RID-CPA RS-IBE,A (λ, T,N), *where* q *is the maximum numberof secret key queries and decryption key queries, and* T = 2ℓ *is the total number of time periods.*

➢ Implementation

To show the practical applicability of the proposed RSIBE scheme, we further implement it using codes from
the Pairing-Based Cryptography library version 0.5.14 . Specifically, we use the symmetric supersingular curve y2 = x3 + x, where the base field size is 512-bit and the embedding degree is 2. The implementation is taken on a Linux-like system (Win7 + MinGW) with an Intel(R) Core(TM) i5 CPU (650@3.20GHz) and 4.00 GB RAM.

V.CONCLUSIONS

Cloud computing brings great convenience for people. Particularly, it perfectly matches

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 21, August 2017

the increased need of sharing data over the Internet. In this paper, to build a cost-effective and authentic data sharing system in cloud computing, we proposed a notion called RS-IBE, which supports identity revocation and ciphertext update simultaneously such that a revoked user is prevented from accessing previously shared data, as well as subsequently shared data. Furthermore, a concrete construction of RS-IBE is presented. The proposed
RS-IBE scheme is proved adaptive-secure in the standard model, under the decisional ℓ-DBHE assumption. The comparison results demonstrate that our scheme has advantages in terms of efficiency and functionality, and thus is more feasible for practical applications.

VI.References:

[1] L. M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, "A
break in the clouds: towards a cloud definition," *ACM SIGCOMM Computer Communication Review*, vol. 39, no. 1, pp. 50–55, 2008.

[2] iCloud. (2014) Apple storage service.[Online]. Available: https://www.icloud.com/

[3] Azure. (2014) Azure storage service.[Online]. Available: http://www.windowsazure.com/

[4] Amazon. (2014) Amazon simple storage service (amazon s3). [Online]. Available: http://aws.amazon.com/s3/

[5] K. Chard, K. Bubendorfer, S. Caton, and O. F. Rana, "Social cloud
computing: A vision for socially motivated resource sharing," *Services Computing, IEEE Transactions on*, vol. 5, no. 4, pp. 551–563,2012.

[6] C. Wang, S. S. Chow, Q. Wang, K. Ren, and W. Lou, "Privacypreserving
public auditing for secure cloud storage," *Computers, IEEE Transactions on*, vol. 62, no. 2, pp. 362–375, 2013.

[7] Christo Ananth, M.Danya Priyadharshini, "A Secure Hash Message Authentication Code to avoid Certificate Revocation list Checking in Vehicular Adhoc networks", International Journal of Applied Engineering Research (IJAER), Volume 10, Special Issue 2, 2015,(1250-1254)

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 21, August 2017

[8] M. Bellare and S. K. Miner, "A forward-secure digital signature scheme," in *Advances in Cryptology–CRYPTO 1999*. Springer, 1999, pp. 431–448.

[9] M. Abdalla and L. Reyzin, "A new forward-secure digital signature scheme," in *Advances in Cryptology–ASIACRYPT 2000*. Springer, 2000, pp. 116–129.

[10] A. Kozlov and L. Reyzin, "Forward-secure signatures with fast key update," in *Security in communication Networks*. Springer, 2003, pp. 241–256.

[11] X. Boyen, H. Shacham, E. Shen, and B. Waters, "Forward-secure signatures with untrusted update," in *Proceedings of the 13th ACM conference on Computer and communications security*. ACM, 2006, pp. 191–200.

[12] J. Yu, R. Hao, F. Kong, X. Cheng, J. Fan, and Y. Chen, "Forwardsecure identity-based signature: security notions and construction," *Information Sciences*, vol. 181, no. 3, pp. 648–660, 2011.