International Journal of Electronics Engineering (ISSN: 0973-7383)
Volume 10 • Issue 2 pp. 77-81 June 2018-Dec 2018 www.csjournals.com

RS-IBE: An Advanced Mechanism for Secure Data Sharing In Cloud

Malavika.J, RAVI.G[2]
[1]M.Tech Scholar, CSE dept, MRCET, Hyderabad, India
[2]Assoc. Professor, CSEdept, MRCET, Hyderabad, India

Abstract: Cloud computing would be one of technologies which is going to play a vital role in the next generation of computer engineering field. The increased scalability and flexibility provided by the cloud computing has reduced the costs to a greater extent and therefore the technology has gained wide acceptance. The facility of Data outsourcing in the clouds enables the owner of the data to upload the data and other users can access the same. But, the data stored should be secure in the cloud servers. The data owner has lot of concern about security aspects present with the cloud computing. The data owners hesitate to adopt cloud computing services because of privacy protection issues of data and security of data. The proposed research work aims to undertake the critical issue of identity revocation wherein outsourcing computation into IBE has been introduced for the first time and a revocable IBE scheme in the server-aided setting has been proposed. This scheme offloads most of the key generation related operations to a Key Update Cloud Service Provider for key-issuing and key-update processes. Only a constant number of simple operations for PKG and users are left to perform locally. Data security is provided by using encryption, user authentication; re-encryption in the proposed data storage security model. The proposed system has also introduced outsourcing computation into IBE revocation, formalizes the security definition of outsourced revocable IBE for the first time to the best of our knowledge. Finally, experimental results have demonstrated the efficiency of the proposed construction.
Index Terms: Cloud computing, data sharing, revocation, Identity-based encryption, cipher text update, decryption key exposure.

I. INTRODUCTION

Cloud computing is a model which enables the users for storing the data and programs and accessing them easily through an internet instead of using some hardware and software components in the computer. A cloud computing also have many definition based on their different types of models. The cloud models are classified as the deployment and service models. Cloud users will easily access the applications and data content that stored in the cloud from anywhere in the world by the financial model called as pay-as-you-go. Whenever the data is stored in the cloud there may be problem of security issues and once when the data is outsourced to cloud the cloud provider should check for the data content and the information regarding to the privacy and according to that provided information the provider must provide the security. For the purpose of security different attributes based encryption schemes are used for encryption before outsourcing the data to the cloud server. With authentication and authorization the user can secure the data in the cloud. The data stored in cloud will be usually stored in the pool and where it tries to provide security to those user data content.

A. Outsourcing Data in Cloud

Outsourcing is a familiar method where the third party executes some function for the sake of the company, frequently for the IT department which do not have the resources to undertake. It is an important method for the global information sharing. One of the important services in outsourcing is the database outsourcing during this process the data must be secured from the hackers.

B. Cryptography

Cryptography is a method which is used for storing and transforming the data in the particular form so that only the intended users can read or process the data easily. Cryptography access control is a commonly used technique for the purpose of securing the data on the entrusted servers. Usually when we use this kind of servers then the sensitive data is encrypted before outsourcing the data and the decryption keys will be given only to the approved users and only by using these keys they can decrypt the data without these keys even the servers are not able to decrypt the data. Cryptography is usually classified into 3 different phase they are as follows:

A. Secrete key cryptography.

B. Public key cryptography.
C. Hash function cryptography.

A. Secrete Key Cryptography
A single key will be used by both the user and the receiver here the user contains a key for the data encryption then a similar key will be used by the receiver to decrypt the data hence both users share the same key for encryption and decryption.

B. Public Key Cryptography
In this it consists of two keys the one key will be used by the sender and the receiver to secure the data and other key between the receiver and the sender to insecure the provide data content.

C. Hash Function Cryptography
In this it does not contain any key pairs instead it uses the hash values which will be processed on the basis of the text message content. It is used to check whether the sent data is not altered by others and the data is not affected by the virus. In cryptography we have various methods:

- Substitution methods.
- Reciprocal methods.
- Symmetric methods.
- Asymmetric methods.

The security for the data can be most commonly done by using the Asymmetric method and this method is also called as the public-key method. In this method the key holder will be provided with two keys the public key and the private key content.

C. Encryption and Decryption

For the purpose of securing the data in cloud we use the encryption and decryption methods. The security for the data can also be done using the following phases:

D. Generating the Keys and Authentication Method

Users are said to store their id secretly because it acts as a tool to verify the user every time when they login to the system. The valid users have some id/password combinations for the purpose of providing the security to their data. The authentication can be done through biometrics were we look into fingerprint, voice face, keyboard timings of the users. The authentication can also be done by cipher text content. The cipher text is an encrypted text where the data result will be obtained in an encrypted format. The data owner's identification, significance and the key (master/public) of the data owners attributes will be contained in the cipher class content.

E. Key Aggregation

When data is shared over the distributed cloud environment it can be secured by providing the aggregate key. For the particular data owners the aggregate key consists of some identity to find the perfect identifier along with the attribute based modules. This key is usually used to share the data between each other using some secret keys in between them. Key aggregation authorizes the users/data provider to share data with others in a confident way by using some small cipher text expansion, and this text can be provided to each authorized users by providing a single and small aggregate keys. These aggregate key can be sent to the authorized user through any means of communication mode secretly, the communication mode can be via email, SMS etc. This aggregate key helps the other user to decrypt the data.

II. KEY REVOCATION PROCESS

Revocation means recall. By public key infrastructure and Certificate Revocation List (CRL) the revocation operation can be done in cryptosystem. The CRL contains a list of certificate that is revoked. Firmly removing the compromised keys can be done by revocation process. Based on the data owners id the keys/data are revoked in cloud. When the master key content and the public key content are redefined then the revocation event will be called related to their variable attribute and later by using the master key the data will be re-encrypted.

A. Proxy re-encryption and Identity Based Encryption (IBE)
The secure communication can be done in the public key cryptography when both the sender and receiver tries to create a encryption and signature key pairs to the data content that has to be secured and then submit the certificate request to the Certificate Authority (CA) along with the proof of identity and then receive the CA-signed certificate which is used for validation and then later they exchange the encrypted message. This process was time consuming and to out come from this process the identity based encryption was introduced. This as the following advantage:

1. In IBE system we use strings such as email address or IP address are used for the public key to the user content instead of issuing certificate or revocation keys.

2. Users does not store any additional decryption key in proxy re-encryption, i.e only by using the users own secret keys the decryption process will be completed.

International Journal of Electronics Engineering (ISSN: 0973-7383)
Volume 10 • Issue 2 pp. 77-81 June 2018-Dec 2018 www.csjournals.com

III. EXISTING AND PROPOSED SYSTMS

3.1 Existing System

Natural revocation way for IBE is proposed in this 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.

3.1.1 Disadvantages

- It's not scalable.
- It's not secure.

3.2 Proposed System

We introduce a notion called revocable storage identity-based encryption (RS-IBE) for building a cost-effective data sharing system that fulfills the three security goals. More precisely, the following achievements are captured in this paper:

• We provide formal definitions for RS-IBE and its corresponding security model;
• We present a concrete construction of RS-IBE. The proposed scheme can provide confidentiality and backward/forward2 secrecy simultaneously;
• We prove the security of the proposed scheme in the standard model, under the decisional ℓ-Bilinear Diffie-Hellman Exponent (ℓ-BDHE) assumption. In addition, the proposed scheme can withstand decryption key exposure;

3.2.1 Advantages

- The procedure of cipher text update only needs public information.
- The additional computation and storage complexity, which are brought in by the forward secrecy.

3.3 Architecture

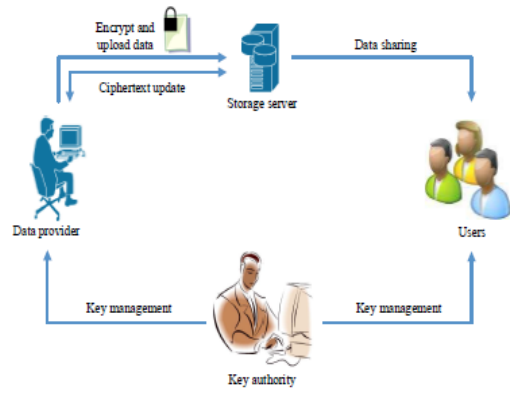


Fig.1. System Architecture

IV. PERFORMANCE DISCUSSIONS

In this section, we discuss the performance of the proposedRS-IBE scheme by comparing it with previous works interms of communication and storage cost, time complexityand functionalities, which are summarized in Table 1,Table 2 and Table 3.

From Table 1we can see that the sizes of private keyand update key in schemes and our scheme areall upper bounded by $O(r\log N/r)$, since these schemes allutilize binary data structure to achieve revocation. On theother hand, Liang et al.'s scheme involves a broadcastencryption scheme to distribute update key such that theirscheme has constant sizes of private key and update key.Furthermore, by delegating the generation of re-encryptionkey to the key authority, the cipher text size of their schemealso achieves constant. However, to this end, the key authorityhas to maintain a data table for each user to store theuser's secret key for all time periods, which brings $O(T)\,\tau_{G1}$

TABLE 1
Comparisons of communication and storage cost with previous works

Schemes	Private key size	Update key size	Ciphertext size
Libert and Vergnaud [22]	$O(\log N)\tau_{G_1}$	$O(r\log N/r)\tau_{G_1}$	$O(1)\tau_{G_1}+O(1)\tau_{G_2}$
Seo and Emura [24]	$O(\log N)\tau_{G_1}$	$O(r\log N/r)\tau_{G_1}$	$O(1)\tau_{G_1}+O(1)\tau_{G_2}$
Liang et al. [26]	$O(1)\tau_{G_1}$	$O(1)\tau_{G_1}$	$O(1)\tau_{G_1}+O(1)\tau_{G_2}$
Our scheme	$O(\log N)\tau_{G_1}$	$O(r\log N/r)\tau_{G_1}$ ‡	$O(\log(T)^2)\tau_{G_1}+O(1)\tau_{G_2}$

* τ_{G_1} and τ_{G_2} are the sizes of group elements in G_1 and G_2, respectively. N is the maximum number of system users. r is the number of revoked users. T is the total number of time periods.
‡ In fact, it is $O(r\log(N/r))$ when $1 \le r \le N/2$, and $O(N-r)$ when $N/2 < r \le N$.

TABLE 2
Comparisons of time complexity with previous works

Schemes	Encryption	Decryption	CTUpdate
Libert and Vergnaud [22]	$O(1)e+O(1)p$	$O(1)p$	0
Seo and Emura [24]	$O(1)e+O(1)p$	$O(1)p$	0
Liang et al. [26]	$O(1)e+O(1)p$	$O(1)p$	$(O(N))e+O(1)p$
Our scheme	$O(\log T)e+O(1)p$	$O(1)p$	$O(\log(T)^2)e+O(1)p$

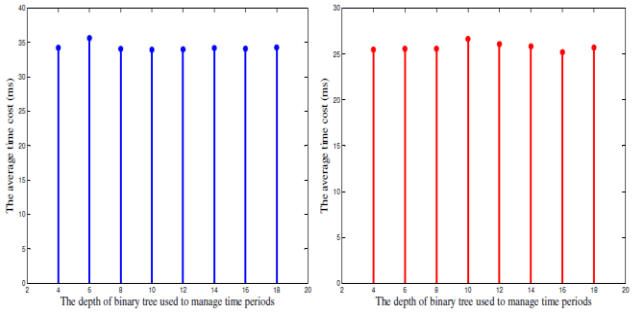
* p and e indicate the cost of performing a bilinear pairing and exponentiation.

TABLE 3
Comparisons of security and functionality with previous works

International Journal of Electronics Engineering (ISSN: 0973-7383)
Volume 10 • Issue 2 pp. 77-81 June 2018-Dec 2018 www.csjournals.com

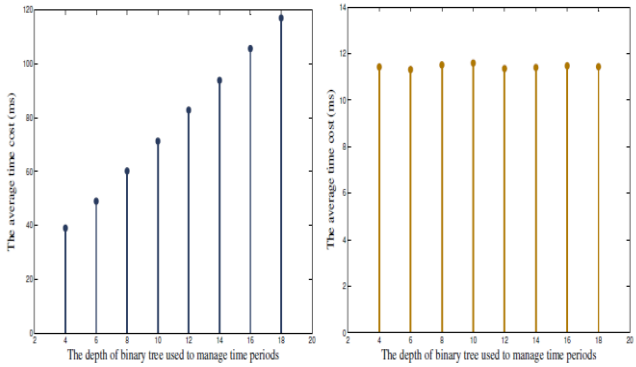
Schemes	Model	Assumption	PKU	PCU	CA	DKE	FS	BS
Libert and Vergnaud [22]	Adaptive	DBDH	√	x	√	x	√	x
Seo and Emura [24]	Adaptive	DBDH	√	x	√	√	√	x
Liang et al. [26]	Adaptive	DBDH	x	x	x	√	√	√
Our scheme	Adaptive	ℓ-dBDHE	√	√	√	√	√	√

* Adaptive means an adaptive-secure model. DBDH is Decisional Bilinear Diffie-Hellman assumption, and ℓ-dBDHE is decisional ℓ-Bilinear Diffie-Hellman Exponent assumption. CA is collusion attack. DKE is decryption key exposure. FS and BS indicate forward and backward secrecy, respectively.



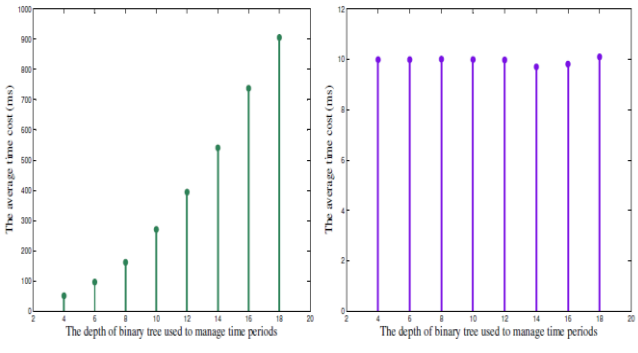
(a) PKGen (b) KeyUpdate

Fig.2. The time costs of the algorithms PKGen and KeyUpdate.



(a) Encrypt (b) DKGen

Fig.3. The time costs of the algorithms Encrypt and DKGen.



(a) CTUpdate (b) Decrypt

Fig.4. The time costs of the algorithms CTUpdate and Decrypt.

storage cost for the key authority. Conversely, the cipher textsize of our scheme is just linear in log $(T)^2$. In addition, wenote that in all listed schemes, the private key generatorneeds to periodically produce an update key, it must beonline if each time period is rather short, e.g., an hour.However, from the perspective of practical applications, thefrequency of updating users' decryption keys should notbe too small. A time period like a week, half a month or amoth is more desirable. As a consequence, the private keygenerator just needs to produce an update key for the nextperiod when the current time period is over. Thus the PKGdoes not need to be always online. Another limitation ofthese listed schemes is that the generated cipher text has thesize linear with the number of receivers. To overcome thisissue, a natural manner is to construct a similar scheme inthe setting of broadcast encryption.

On the aspect of time complexity, as illustrated inTable 2, the enumerated schemes all have constant time of decryption. For two schemes supporting cipher text update,the time complexity of cipher text update in Liang et al.'sscheme is linear in N since the key authority needs toproduce a re-encryption key for each user to re-encryptthe cipher text. However, the time complexity of cipher textupdate in our scheme is linear in $\log(T)^2$.As shown in Table 3, the four schemes are all provedsecure in an adaptive-secure model, and can also providebackward secrecy since they all supports identity revocation.

But the security of our scheme is built upon a relativelystrong security assumption, decisional ℓ-DBHE assumption.
The schemes and ours update user's secret keysin a public way, namely, the update key is available forall users. However, Liang et al.'s scheme involves themethod of broad encryption to update user's secret keysuch that only non-revoked users can obtain the update key.Consequently, their scheme cannot resist collusion attack ofrevoked users and non-revoked users. Compared with theschemes and, Liang et al.'s scheme and ourscan both provide forward secrecy by additionally introducingthe functionality of cipher textupdate? But the procedureof cipher text update in Liang et al.'s scheme isperformed in a private and interactive way, since it requiresthe key authority to periodically produce and provide re-encryptionkeys for the cloud server to update cipher text.However, in our schemes, the cloud server itself can updatecipher text by just using public parameter.

4.1 Implementation

To show the practical applicability of the proposed RSIBEscheme, we further implement it using codes fromthe Pairing-Based Cryptography library version 0.5.14.Specifically, we use the symmetric super singular curve$y^2 = x^3 + x$, where the base field size is 512-bit andthe embedding degree is 2. The implementation is takenon a Linux-like system (Win7 + MinGW) with an Intel(R)Core(TM) i5 CPU (650@3.20GHz) and 4.00 GB RAM.

In the implementation, we set the number of users tobe N= 8 and the revoked uses to be R= 4 (the nodesη_2, η_3, η_4, η_7 are revoked). In Fig.2, Fig.3 and Fig.4, we present the running time of the basic algorithms,i.e., **PKGen**, **KeyUpdate**, **DKGen**, **Encrypt**, **CTUpdate**and **Decrypt**, for different choice of the total number oftime periods $T\in$ $\{2^4, 2^6, 2^8, 2^{10}, 2^{12}, 2^{14}, 2^{16}, 2^{18}\}$. To generatethe experimental results, we perform as the followingprocedure: generate the private key and encrypt a messageat the initial time period, then, periodically update the privatekey and the cipher text, and decrypt the cipher text. For asmall number of time periods: $T\in$ $\{2^4, 2^6, 2^8\}$, the runningtime of each algorithm is obtained by computing the averageof running the above procedure 100 times. While, for alarge number of time periods: $T\in$ $\{2^{10}, 2^{12}, 2^{14}, 2^{16}, 2^{18}\}$,the running time for each algorithm is obtained by runningthe above procedure only once, and the running time forupdate algorithm is the mean of the first 512 time periods.We observe that, the time costs of the algorithms **PKGen**, **KeyUpdate**, **DKGen** and **Decrypt** are independent of thetotal number of time periods, and no more than 40 milliseconds.On the other hand, it takes less than 1 second for theuser to initially encrypting the message, which would beshare on the cloud. Although the time cost of the algorithm**CTUpdate** is apparently greater than other algorithms, itis run by a cloud server with powerful capability of computation.Thus, our RS-IBE scheme is feasible for practicalapplications.

V. CONCLUSION

Cloud computing is a distributed system connected with the servers where users can share data each other. An Identity-based proxy re-encryption scheme has been introduced to outsource the sensitive data from the main user to the external user. Nevertheless, they cannot be employed in cloud computing. This system will increase the security by introducing the identity based secure encryption and re-encryption process for the stored data. This work has concentrated on the identity revocation. It has used outsourcing calculation in the IBE and suggested in a revocation scheme where in the revocation operation is delegated in CSP. The proposed system achieves the following:

1. It provides constant efficiency to compute the PKG and size of private key at the user.

2. It offers convenience since the user may not contact the PKG at the time of key updating and there is no need of user authentication between the user and the CSP.

VI. REFERENCES

[1] Jianghong Wei, Wenfen Liu, Xuexian Hu, “Secure Data Sharing in Cloud Computing UsingRevocable-Storage Identity-Based Encryption”, Journal of Latex Class Files, Vol. 14, No. 8, August 2015.

[2] L. M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, “Abreak in the clouds: towards a cloud definition,” ACM SIGCOMMComputer Communication Review, vol. 39, no. 1, pp. 50–55, 2008.

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

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

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

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

[7] C. Wang, S. S. Chow, Q. Wang, K. Ren, and W. Lou, “Privacypreservingpublic auditing for secure cloud storage,” Computers,IEEE Transactions on, vol. 62, no. 2, pp. 362–375, 2013.

[8] G. Anthes, “Security in the cloud,” Communications of the ACM,vol. 53, no. 11, pp. 16–18, 2010.

[9] K. Yang and X. Jia, “An efficient and secure dynamic auditing protocolfor data storage in cloud computing,” Parallel and DistributedSystems, IEEE Transactions on, vol. 24, no. 9, pp. 1717–1726, 2013.

[10] B. Wang, B. Li, and H. Li, “Public auditing for shared datawith efficient user revocation in the cloud,” in INFOCOM, 2013Proceedings IEEE. IEEE, 2013, pp. 2904–2912.

[11] S. Ruj, M. Stojmenovic, and A. Nayak, “Decentralized accesscontrol with anonymous authentication of data stored in clouds,”Parallel and Distributed Systems, IEEE Transactions on, vol. 25, no. 2,pp. 384–394, 2014.

[12] X. Huang, J. Liu, S. Tang, Y. Xiang, K. Liang, L. Xu, andJ. Zhou, “Cost-effective authentic and anonymous data sharingwith forward security,” Computers, IEEE Transactions on, 2014, doi:10.1109/TC.2014.2315619.