International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 4 Issue 2, February 2020 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Efficient and Enhanced Proxy Re-Encryption Algorithm for Skyline Queries

K. Kalaivani

M.E, Department of CSE, SNS College of Engineering, Coimbatore, Tamil Nadu, India

ABSTRACT

Identity-based encryption (IBE) is a very attractive cryptographic primitive due to its unnecessity of any certificate managements. Nevertheless, the user revocation problem in IBE remains an elusive research problem and hence, it is an important research topic. One possible approach in achieving revocations is to update user's decryption keys. However, to avoid the need of secret channels, public time keys need to be issued to allow this update to occur. It is unfortunate that this method often suffers from two problems: 1) the user has to maintain linearly growing decryption keys; and 2) the revoked users can still access ciphertexts prior to revocation. At the first glance, proxy re-encryption technique may provide a solution to this problem, but the ciphertexts will become longer after each re-encryption, which makes it impractical. In this paper, we present a revocable identity-based encryption scheme with cloud-aided ciphertext evolution. Our construction solves the two aforementioned problems via ciphertext evolution implemented by the cloud. Additionally, the size of ciphertexts in the cloud remains constant size regardless of evolutions. The scheme is provably secure against chosen-ciphertext attacks based on the BDH problem. The comparisons with the existing related works show that our scheme enjoys better efficiency, thus is practical for the data sharing in cloud storage.

How to cite this paper: K. Kalaivani "Efficient and Enhanced Proxy Re-Encryption Algorithm for Skyline Queries" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-4 | Issue-2, February 2020, pp.1141-1144, URL: www.ijtsrd.com/papers/ijtsrd30294.pdf

IJTSRD30294

Copyright © 2019 by author(s) and International Journal of Trend in Scientific Research and Development Journal. This is an Open Access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0) (http://creativecommons.org/licenses/by/4.0)

International Journal of Trend in Scientific Research and Development ISSN: 2456-6470

INRODUCTION

PUBLIC key encryption (PKE) provides an excellent solution to the problem of key distribution in symmetric key. An important issue in PKE is the authenticity of user public keys. The traditional PKE authenticates user public key via releasing certificates. Nevertheless, the certificate management is a heavy burden to the public key system, which is the primary drawback in PKE. To overcome this drawback, Shamir set forth a new notion called "Identity based public key cryptography" in 1984. This public key cryptosystem employs every user's unique identity as its public key. Therefore, the authenticity of this public key is no longer questionable, and hence, there is no certificate required. Since the first practical identity-based encryption (IBE) scheme was presented by Boneh and Franklin in 2001 [3], IBE has attracted a lot of attentions from both academia and industry.

To date, there have been many IBE schemes proposed in the literature. One important issue to make identity-based encryption practical is the user revocation. This problem was first discussed in BF's seminal work. As stated earlier, different from the traditional public key system, there is no certificate in identity-based system. Therefore, the conventional user revocation technique is not applicable to the identity-based systems. Actually, the user private key can be viewed as an implicit certificate. Boneh and Franklin suggested that the PKG periodically issues new private keys by attaching time tags for non-revoked users. The user revocation can be launched by the PKG stoping the issuing of new user private keys with the time tags. Unfortunately, this revocation system is very impractical, because the PKG has to carry heavy overhead (O(n) where n is the number of non-revoked users), especially for the establishing of secret channels. Boldyreva et al. presented the first scalable revocable IBE scheme in 2008 their scheme, only public channels are required for the key updating. Furthermore, they utilized the complete subtree to realize a logarithm growth O(log(n)) of key-updating with non-revoked users.

With this approach of revocation method, many revocable identity-based encryption (RIBE) schemes have been proposed. However, when taking these schemes in some application scenarios, some problems arise. Let's consider the scenario of secure data sharing in cloud storage by applying a revocable identity-based encryption. Suppose there are four entities involved, namely the data owner, the data user, the cloud server and the PKG. To our best knowledge, the existing schemes suffer from two shortcomings or at least one of them.

The data user needs to utilize the time key TKID as well as the private key to decrypt a ciphertext encrypted at the time t. So, the data user has to maintain all the time keys (O(t)) (or decryption keys computed from time keys) for different time-period decryptions. This consumes a lot of storage resources for data users, thus it is very impractical especially in source-limited environments.

When a user is revoked by the PKG for such as private key compromise or expiring, the user can still decrypt those ciphertexts prior to revocation in the cloud.

Though some works do not have these problems, they suffer from new problems: the ciphertexts grow longer with the number of ciphertext-transformation (the basic construction), or the costly computation and communication of reencryption keys between the user and the server. We give a new and efficient RIBE scheme that can solve the two problems. As shown in Fig. 1, the cloud server helps a ciphertext C uploaded by the data owner evolve to a new one C0; then the data user decrypts the ciphertext by employing merely its current time key as well as private key. So, the data user only needs to keep one time key – the current time key; and the revoked data user cannot access any ciphertext including those before revocation; no matter how many times a ciphertext in the cloud evolves, the length of the ciphertext remains unchanged; different to proxy re-encryption, no computation or communication is needed for the re-encryption keys.

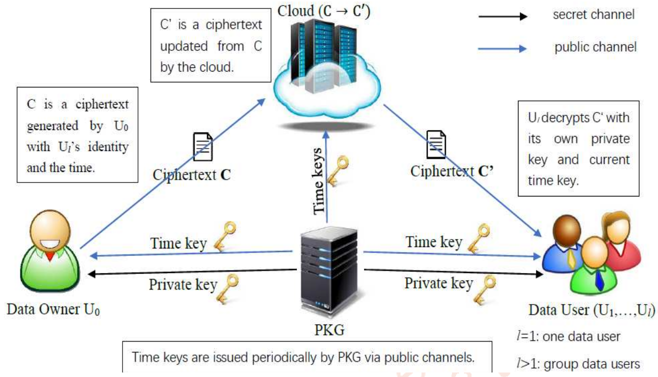

Cloud (C → C′)
C' is a ciphertext updated from C by the cloud.
secret channel
public channel
C is a ciphertext generated by U₀ with U_l's identity and the time.
Ciphertext C
Time keys
Ciphertext C'
U_l decrypts C' with its own private key and current time key.
Time key
Private key
Time key
Private key
Data Owner U₀
PKG
Data User (U₁,…,U_l)
l=1: one data user
l>1: group data users
Time keys are issued periodically by PKG via public channels.

Figure1: overall architecture

RELATED WORKS:

Boldyreva et al. first presented a scalable revocable IBE scheme in 2008. The complete subtree structure is used to obtain a logarithm growth of updating key. This work was subsequently improved in with strong security. In 2013, Seo and Emura introduced decryption-key-exposure threat and presented a revocable IBE scheme that can resist decryption-key-exposure. Sun et al. extended Seo et al.'s scheme to the certificate less setting. In 2017, Watanabe et al. gave a new revocable and decryption key-exposure resistent IBE scheme. The scheme has short public parameters in prime-order groups. A very recent work showed a revocable hierarchical identity-based encryption scheme.

Unfortunately, almost all these RIBE works suffer from the two drawbacks mentioned above especially in the applications like cloud storage. In 2014, Liang et al. employed proxy re-encryption technique to construct a revocable identity-based encryption scheme. Their scheme solves the two problems by re-encrypting ciphertexts in the cloud. However, the ciphertexts become longer and longer with the number of re-encryption. improved Liang et al.'s scheme on the efficiency but suffers from increasing list of decryption keys for different-period ciphertexts. and pointed out the security weakness of Liang et al.'s scheme against collusion attacks. Other related works are such as In these works, the revocation is implemented by a third party e.g. the cloud server. Identity-based public key cryptography (ID-PKC) was introduced by Shamir in 1984. It is a good alternative for traditional PKC which requires high maintenance cost for certificate management. However, ID-PKC is easy to suffer from the private key escrow. To avoid this drawback, Al-Riyami and Paterson introduced the certificateless public key cryptography (CLPKC) in 2003. The CLPKC combines the advantages of ID-PKC and traditional PKC because it has no key escrow and at the same time alleviates the certificate management. At present, a large number of encryption and signature schemes are proposed in CLPKC. We refer readers to works. In a public key cryptosystem, an vital issue is howto revoke a user when his/her private key is leaked or the permission is expired. In traditional PKC, there exist some ripe revocation methods, such as Certificate Revocation List (CRL), online certificate status protocol (OCSP) and a revocation technique proposed by Novomodo. In ID-PKC and CLPKC, the initial revocation technique is that the KGC periodically updates the (partial) private key for the user. However, each new key must be transmitted to the user through a secret channel. And the establishment of secret channel requires a lot of calculations by the system and the users, which greatly increases the communication overhead. Therefore, it is better to use public channels instead of secret channels when designing a revocation scheme. As matters stand, many revocation schemes with public channels have been proposed in ID-PKC. In 2008, Boldyreva et al. presented an ID-based encryption scheme with efficient revocationn. In 2012, Tseng and Tsai and Tsai et al. constructed a revocable ID-based encryption scheme and a revocable ID-based signature scheme with batch verifica-tions. In 2013, Seo and Emura proposed a revocable ID-based encryption scheme against decryption exposure

Existing system

In contrast to traditional solutions, where the IT services are under proper physical, logical and personnel controls, Cloud Computing moves the application software and databases to the large data centers, where the management of the data and services may not be fully trustworthy. This unique attribute, however, poses many new security challenges which have not been well understood

PROPOSED SYSTEM

We focus on cloud data storage security, which has always been an important aspect of quality of service. To ensure the correctness of users' data in the cloud, we propose an effective and flexible distributed scheme with two salient features, opposing to its predecessors. By utilizing the encryption keys our scheme achieves the integration of storage correctness insurance. Unlike most prior works, the new scheme further supports secure and efficient dynamic operations on data blocks, including: data update, delete and append.

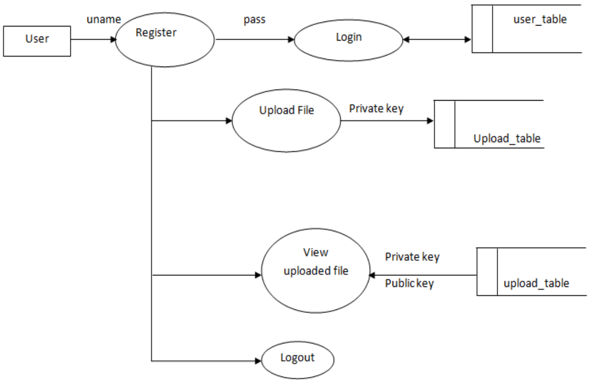


Figure1: Data Owner Module

Before logging to the cloud, user has to register their details like user id, password. This registration will used to avoid anonymous users. By this user will get a user name and password for their account. Every user must be register then only they can log in the cloud.

After that user enter their user name and password what they registered. After log in to cloud user can manage their cloud data.

Now user can upload the file to cloud, for each files uploaded, random private key is generated and these private keys will encrypt the uploaded file and gets stored in cloud. TripleDES encryption algorithm is used. User can view the encrypted file that is stored in cloud. User can select the available Cloud Service Provider and store the data in cloud.

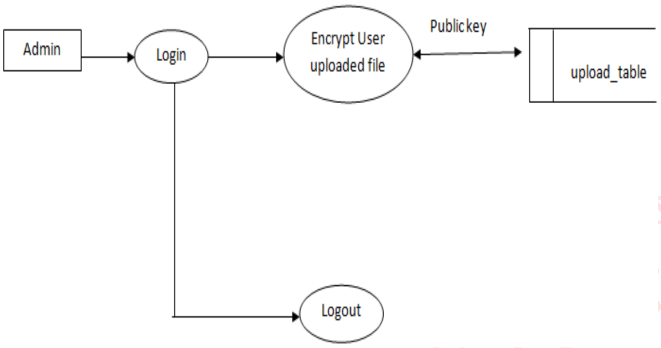
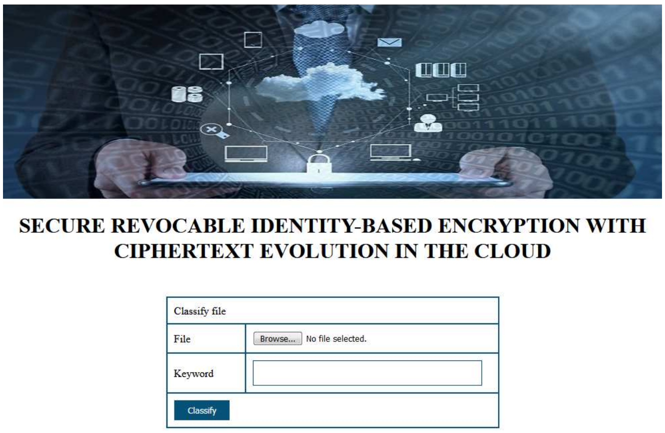


Figure2: Cloud Admin module

Cloud Service Provider enter their user name and password. After log in to cloud, for each user files uploaded, random time variant public key is generated and these public keys will encrypt the uploaded user encrypted file and gets stored in cloud. TripleDES encryption algorithm is used. Cloud Service Provider can view the encrypted file that is stored in cloud.

Cloud Service Provider will specify the time by which file need to be accessed, user who is going to access the file, admin can also view the available user files that are allotted to them. He can't view other Cloud Service Provider files. Now user can view the original uploaded file by specifying time variant public key given for specific uploaded file by Cloud Service Provider. Once again user has to enter Private Key given for specific uploaded file. Here double decryption is done to get the original data. If a hacker gets the access to uploaded file, only encrypted data will be shown to him, instead of original data.



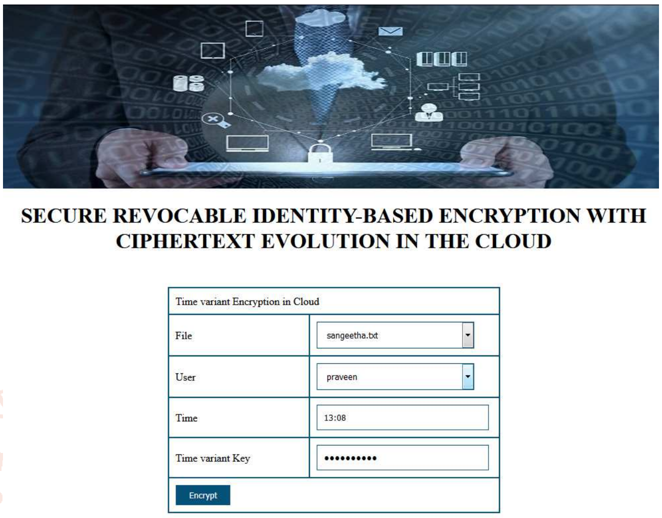
SECURE REVOCABLE IDENTITY-BASED ENCRYPTION WITH CIPHERTEXT EVOLUTION IN THE CLOUD

Classify file

File	Browse... No file selected.
Keyword	

Figure3: Upload File

We construct a revocable identity-based encryption scheme with (cloud-aided) ciphertext evolution (RIBE-CE). Our scheme is proved secure against chosen ciphertext attacks based on the hardness of the BDH problem in the random oracle model. Taking a security parameter k as input, this algorithm outputs a master secret key msk and public parameters params. Private-Key-Extract(params; msk; ID): Taking params, msk and an identity ID as input, this algorithm outputs a private key SKID, which is transmitted to the user via a secret channel. It is run by the PKG.



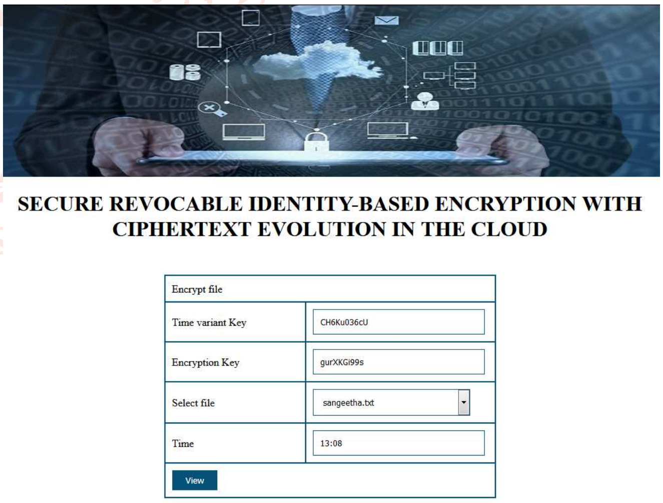
SECURE REVOCABLE IDENTITY-BASED ENCRYPTION WITH CIPHERTEXT EVOLUTION IN THE CLOUD

Time variant Encryption in Cloud

File	sangeetha.txt
User	praveen
Time	13:08
Time variant Key	••••••••••

Figure4: File Encryption

Time-Key-Update(params; msk; ID; t): Taking params, msk, an identity ID and a time tag t as input, this algorithm outputs a time key TKID;t, which is transmitted to the user via a public channel. It is run by the PKG.



SECURE REVOCABLE IDENTITY-BASED ENCRYPTION WITH CIPHERTEXT EVOLUTION IN THE CLOUD

Encrypt file

Time variant Key	CH6Ku036cU
Encryption Key	gurXKGi99s
Select file	sangeetha.txt
Time	13:08

Figure5: File Decryption

Encrypt (params; ID; t; M): Taking params, ID, t and a message M as input, this algorithm outputs a ciphertext C. It is run by the data owner.

Decrypt (params; SKID; TKID; t): Taking params, SKID, TKID; t and C as input, this algorithm outputs a message M or a failure symbol. It is run by the data user.

This application implements cloud server-enabled user revocation, presenting an choice but greater efficient solution to the user revocation problem in the context of fine-grained encryption of cloud data. Meanwhile, this strategy offers speedy access to on-demand services with high availability and scalability. However, to avoid the need of secret channels, public time keys need to be issued to allow this update to occur. Consequently, it is vital to undertake comparatively cheaper solutions to overwrite or replace traditional systems. The scheme exploits the properties of the modular inverse to generate a probabilistic trapdoor which facilitates the search over the secure inverted index table. Users with limited computing power are however more probable to delegate the mask of the decryption task to the cloud servers to reduce the computing cost.

CONCLUSION AND FUTURE WORK

Security is a major requirement in cloud computing when we talk about data storage. Information needs protection, there are many Security Threats, and different types of security risks need to be discussed. In order to improving the security and protection and building the Secure Cloud, There are number of existing techniques used to implement security. we put forward an efficient record storage security in cloud service. The encryption of record permits storing of the record in straightforward and efficient way. Dynamic operations are a further important concept where, encoding and decoding process secures records. It also provides method for flexible access and retrieval. Cost is reduced in data storage. The time and space is also reduced through storage. Also the remote data integrity checking identifies the threats and unruly server while storing the records in cloud guaranteeing data security. We focussed on the user revocation problem in identity-based encryption. One of the efficient revocation methods is to issue time keys periodically via public channels for non-revoked users. We take the scenario of cloud storage as consideration and find that most of the existing works suffer from increasing decryption key list or access ability to ciphertexts prior to revocation. Though the technique of proxy re-encryption can solve the two problems, the length of the ciphertexts grow linearly with the number of cipher text evolutions. Therefore, it is a heavy burden to the server when the data is big. Additionally, the users have to put more computation and communication resource on re-encryption keys. This is not suitable for source-limited applications. In this paper, we presented an efficient solution to the two aforementioned problems simultaneously. The size of a cipher text in the cloud remains constant, no matter how many times the cipher text evolves. The new revocable identity-based encryption with cipher text evolution scheme is constructed by using bilinear parings. The time keys are generated by the PKG periodically and sent to both the user and the cloud. The cloud makes ciphertext evolution by using the time keys. Hence, no extra key computations are involved in our construction. It is efficient for the data sharing application in the cloud. Our scheme enjoys provably strong security against chosen ciphertext attacks based on standard hard problem.

References

[1] A. Boldyreva, V. Goyal, V. Kumar, "Identity-based encryption with efficient revocation," Proc. CCS 2008, ACM, 2008, pp. 417-426

[2] A. Shamir, "Identity-based cryptosystems and signature schemes," Proc. CRYPTO 1984, pp. 47-53.

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

[4] B. Qin, R. H. Deng, Y. Li, S. Liu, "Server-aided revocable identity-based encryption," Proc. ESORICS 2015, LNCS 9326, 2015, pp. 286-304.

[5] D. Boneh, X. Boyen, "Efficient selective-ID secure identity based encryption without random oracles," Proc. EUROCRYPT 2004, LNCS 3027, 2004, pp. 223-238.

[6] D. Boneh, M. Franklin, "Identity-based Encryption from the Weil Pairing," Proc. CRYPTO 2001, LNCS 2139, 2001, pp. 213-229

[7] J. Li, J. Li, X. Chen, C. Jia and W. Lou, "Identity-based Encryption with Outsourced Revocation in Cloud Computing," IEEE Transactions on Computers, 64(2), pp. 425-437, 2015

[8] K. Liang, J. K. Liu, D. S. Wong, W. Susilo, "An efficient cloud-based revocable identity-based proxy re-encryption scheme for public clouds data sharing," In: Kutyowski, M., Vaidya, J. (eds.) ESORICS 2014, Part I. LNCS, vol. 8712, pp. 257-272.

[9] R. Brent, "Efficient identity-based encryption without random oracles," Proc. EUROCRYPT 2005, LNCS 3494, 2005, pp 114-127.

[10] Y. Sun, F. Zhang, L. Shen, R. H. Deng, "Efficient revocable certificate less encryption against decryption key exposure," IET information security, 9(3) (2015) 158-166