International Journal of MC Square Scientific Research Vol.9, No.1 April 2017

REVOCABLE-STORAGE IDENTITY-BASED ENCRYPTION IN CLOUD COMPUTING FOR SECURE DATA SHARING

V.Lasya Reddy [1], B.Ravi Teja [2], 3.Akhil Kumr [3], N. Mahendar kumar [4]
[1, 2, 3, 4] *UG student,*
Department of Computer Science Engineering,
SRM University, Ramapuram, Chennai – 89
[1]lasyareddyvatti@gmail.com, [2]rvtj11@gmail.com
[3]gandediakhilkumar@gmail.com,[4]mahendar.1.kumar@gmail.com

V.Sellam [5]
[5] *Assistant Professor,*
Department of Computer Science Engineering,
SRM University, Ramapuram, Chennai – 89
Mail.id- sellamveera@gmail.com

Abstract— Cloud provides a flexible and convenient way for data sharing, and brings various benefits for both the individual and Organization. A user can directly outsource the shared data to the cloud server, since the data is not highly secured. Here we need to place some crypto graphical enhanced to access the shared data. we are using crypto graphical method called identity based encryption system for sharing the data but it is not static .That is when the user's authorization is expired there should be a mechanism that can remove a person to over the problem .To this end, a notion called revocable-storage identity-based encryption (RS-IBE) is proposed. It can provide the forward/backward security of cipher text by introducing the functionalities of user revocation and cipher text update simultaneously. The revoked user cannot access both old and new shared data. In proposed system have advantages like functionality and cost effective.

Keywords— Cloud computing, Data sharing, Revocation, Identity-based encryption, Cipher text update, Decryption key exposure.

1. Introduction

Cloud computing is model that provides the massive computation capacity and huge memory space .It enables to the user to get access to services irrespective of time and across the multiple platforms which brings great convenient to users . Examples of cloud service providers are a Amazon Ec2, Microsoft azure etc. They provide more flexible and convenient way to share the data over the internet which provides lot of benefits .however it also suffers from lot of security problems which are the primary threat for the cloud users.

Firstly, outsourcing data to cloud usually refers to data is out control of users. This may cause hesitation that out sourced data contains some important and sensitive information.

Secondary is cloud is usually implemented on the open environment so that cloud servers can easily attacked by attackers. Even worse cloud servers itself revels the users data for the illegal profit .Thirdly that data shared in cloud but it is not static .That is when the user's authorization is expired there should be a mechanism that can remove a person from the system. A natural solution for the above problems is we need to place some crypto graphical enhanced to access the shared data. We are using crypto graphical method called identity based encryption system. Further to overcome the security threats, such kind of identity based access control on shared data should follow the following security goals.

1.1 Data confidentiality: unauthorised users should be prevented from access the data that is stored in cloud server. In addition, which is supposed to be honest but curious should also be prevent from knowing plaintext of the shared data

1.2 Backward secrecy:
Back ward secrecy is that when users authorization expire or users secret key is compromised .he/she should be prevented from accessing the previously shared data that are still encrypted under his /her identity

1.3 Forward secrecy: Forward secrecy means is that when user's authorization expires or users secret key is compromised .he/she should be prevented from accessing the shared data that can be previously accessed by him. The specific problem addressed with the paper is how to create a basic identity based crypto graphical tool to achieve the above security goals

1.4 Motivation
It seems that the revocable identity based encryp1tion might be fulfilling the above mentioned security requirements for data sharing. RIBE feature enable the users that the current time period to the cipher text such that the receiver can decrypt the file only under the condition he /she is not revoked at that time period

RIBE based data sharing works as follows

Step 1:
Here data providers first confirm the number of users who can share the data .Then data provider encrypts the data under the identity of the users suppose we take two users such as bob and lee.

Step 2:
When, either the bob or lee wants to get the shared data. He can directly download the shared data and decrypt the corresponding cipher text. However unauthorised users cannot access the shared data

Step 3:

If any of the users revoked or authorization is expired. Data owner download the whole the data and re –encrypt an upload the data in cloud so that unauthorized user cannot access the data .Obviously the data sharing provides the both forward and backward secrecy but the problem is here we are downloading the whole data we decrypting then re- encrypting and uploading the file this take lot of time and it is cost effective. The efficiency of data sharing will be decreased. Another one issue is we will be facing the lot of security problems. Note that the process of decrypt –then re-encrypt involves in users secret key information this make overall data sharing system vulnerable to new attacks. To overcome this problem there is only one method that is cloud server to directly re –encrypt the cipher text of the shared data in addition , the technique of proxy re encryption is also can be used to conquer the aforementioned problem of efficiency.

2. Literature Survey

The concept of identity-based encryption was introduced by Shamir [13] and conveniently instantiated by Boneh and Franklin [2]. It eliminates the use of a public key infrastructure (PKI). Regardless of the setting of IBE or PKI, there will be be an approach to remove users from the system when necessary, e.g., if the authority of the some user is expired or the secret key of some user is not valid . In the traditional PKI setting, the problem of revocation has been well studied [3], [4], [5], [6], [7] and several techniques are widely approved, such as certificate revocation list or appending validity periods to certificates. However, there are only a few studies on revocation in the setting of IBE. Boneh and Franklin [2] first proposed a natural revocation way for the identity based encryption.

They provide the current time period to the CT, and the non-revoked user will get the private keys for each time period from the key authority. Unfortunately, this solution is not scalable, since it requires key authority to perform the linear work. In addition, a secure channel is essential for the key authority and non-revoked users to transmit new keys. To conquer this problem, Boldyreva, Goyal and Kumar [8] introduced a novel approach to achieve efficient revocation. They used a binary tree to manage identity such that their RIBE scheme reduces the complexity of key revocation to logarithmic (instead of linear) in the maximum number of system users.

However, this scheme only achieves selective security. Subsequently, by using the aforementioned revocation technique, Libertand Vergnaud [9] proposed an adaptively secure RIBE scheme based on a variant of Water's IBE scheme [10] Chenet al[11]. Constructed an RIBE scheme, from lattices. Recently, Seo and Emura proposed an efficient RIBE scheme should withstand to a realistic threat called decryption key exposure, which means that the disclosure of decryption key for current time period. It has has no effect on the security of decryption keys for other time periods.

Motivated by the above work and, Liang et al. introduced a cloud-based revocable identity-based proxy re-encryption that supports user revocation and CTU. To reduce the complexity of revocation, they utilized a broadcast encryption scheme[12] to encrypt the cipher text of the update key ,which is independent of users, such that only non-revoked

Forward-secure cryptosystems:

In 1997, Anderson [13] introduced the forward security in the setting of signature to bind the damage of key exposure. The basic idea is splitting the whole life time of a private key into T different time periods, such that it consist of the private key for current time period cannot enable an opponent to produce valid signatures for previous time periods. Subsequently, Bell are and Miner provided formal definitions of forward-secure signature and presented practical solutions.

Since then, a large number of forward-secure signature schemes [14], [15], [16], [17], [18] has been proposed .In the context of encryption, Canetti, Halevi and Katz proposed the first forward-secure, public-key encryption scheme. Specifically they firstly constructed a binary tree\encryption, and it is transformed into the random oracle model. Based on Canetti etal's approach, Yao et al. proposed a forward-secure hierarchical IBE by employing two hierarchical IBE schemes, and Nieto et al. Particularly, by combining Boldy reva et al.'s [8] revocation technique and the aforementioned idea of forwardsecurity1, in CRYPTO 2012 Sahai, Seyalioglu and Waters proposed a generic solution f so-called revocable storage attribute-based encryption, which supports both the user revocation and cipher text update at a time.. In other words, their solution provides both forward and backward secrecy.

What must be pointed out is that the process of cipher text update of this solution only needs PI (Public Information).However, their construction cannot withstand to decryption key exposure, since the decryption is a matching result of private key and update key which is independent of users, such that only non-revoked users can decrypt the update key. However, this kind of revocation method cannot with stand with the collusion of revoked users and mischievous non-revoked users as mischievous non revoked users can share the update key with those revoked users. Furthermore, to update the cipher text, the key authority in their scheme needs to maintain a table for each user to produce the re-encryption key for each time period, which significantly increases the key authority's workload.

3. Proposed Method

To overcome the above mentioned security problems we are implementing the Revocable storage identity based encryption .Revocable storage identity-based encryption (RS-IBE) is useful for building a cost effective and secure data sharing. RS-IBE provides confidentiality and backward/forward secrecy simultaneously. It firstly constructs a binary tree encryption, and then transform it into forward-secure encryption with provable security .This process of updating the cipher text is only need of public information .This construction will not be secure to decrypt key exposure, the decryption is a same result of private key and

update key. Here we are providing the security of proposed system by l-bilinear Diffie Hellman Exponent; it can withstand the decryption key venerability. The algorithms we are using in RSIBE are Boneh-Franklin Identity-based Encryption. Through this algorithm we can overcome the security problems .It consist of following algorithms:

Setup (1λ, N, T): the setup algorithm take the input as security parameter λ, the maximum number of user be N and time period T and it outputs the public parameters and the master key

PKGen (PP,MSK, ID); the private key generator takes the parameters such as the pp and master **k**ey and generates the secret key skd1 for id and updated state

Key Update (PP, MSK, RL, t, st):the key update takes the algorithm takes the parameters PP,MSK ,RL and it outputs KUt.

DKGen (PP, SKid, KUt):the decryption algorithm takes the inputs such as PP, SKid ,KUt and generates the decryption key DKid,for id with time period

CTUpdate (PP,CTid,t,t′) : it takes the parameters as input PP, CTid ,t, DKid ,t′ and the new time period t<T and update the cipher text.

Revoke (PP,RL, ID t, st): The revoke algorithm takes the input such as pp and identity id I to be revoked , current revoked list RL at state st and revocation time period t<T and it updates the RL to new .

3.1 System Modelling:

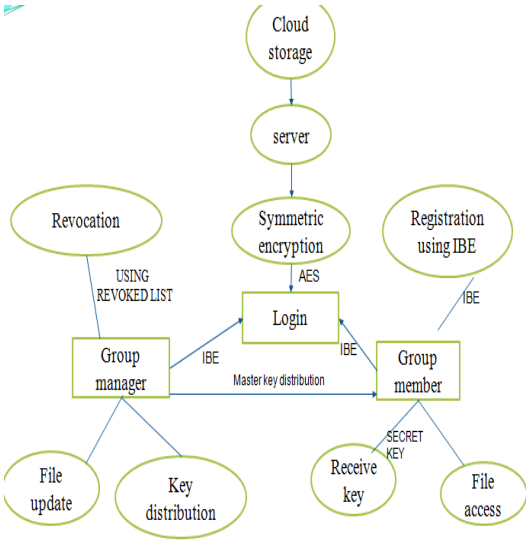

Figure no 1-Architecture Diagram for RS-IBE

3.2 System Implementation

3.2.1 Cloud Storage:-

Cloud is the next stage of evolution of internet. Cloud storage is used to store the data in which the data is maintained, managed, backed up remotely and made available to users. Users generally have to pay for their cloud data storage on a per-consumption, monthly rate. Although the per-gigabyte cost has been radically reduced, cloud storage providers have added operating expenses that can make the technology more expensive than users. Cloud security continues to be a concern among users. Providers have tried to deal with those fears by building security capabilities, such as encryption and authentication, into the services.

3.2.2 Server:-

A server is a device that provides functionality for other programs and devices are called clients. Servers provide various functionalities, such as sharing data or resources among multiple clients, performing computation for a client. A single server can serve multiple clients, and a single client can use multiple servers. A client process can run on the same device or may connect over a network to a server on a different device. Various types of servers are database servers, file servers, mail servers, print servers, web servers, game servers, and application servers. Client–server systems are most frequently implemented by the request–response model: a client sends a request to the server, it performs action and sends a response back to the client, typically with a result or acknowledgement. This often implies that it is more powerful and reliable than standard personal computers, but alternatively, large computing clusters may be composed of many relatively simple, replaceable server components**.**

3.2.3 Symmetric Encryption:-

Symmetric encryption is defined as a process in which the same key is used for both encryption and decryption. Between two communicating parties like sender and receiver use symmetric encryption for secure communication and the key represents a shared secret between two parties. Symmetric encryption is preferred more when compared to asymmetric encryption. Symmetric encryption is often used for bulk data encryption. There are few algorithms which comes under symmetric encryption they are-AES, DES, skipjack etc

3.2.4 Validation:-

It is a portal which is used for logging into a specific page. Each user has a separate login id and password provided. When a user leaves that particular company that particular login id of that user will be deleted. If that particular id is not deleted that person will be able to view the details of that company in order to prevent this we implement a concept called revocable storage identity based encryption.

3.2.5 Authority: -

The authority is the one who allots new user the id and the password. Each user is having a separate or unique signature even if the user id and password of a particular person are known the signature varies so the data cannot be seen. Here the data present in the cloud is secured more precisely.

3.2.6 Group manager:-

The group member has various tasks to perform out of which in order to access a file the group member has to request for the particular file and the authority will allow the access to the requested file and in order to view that the user need the public key of that file and it will sent by the authority. The group member cannot access the data from cloud directly.

4. Conclusion

Cloud computing brings great convenience for people. Particularly, it perfectly matches the increased need of sharing data over the Internet. In this paper, to build a cost-effective and secure data sharing system in cloud computing, we proposed a notion called RS-IBE, which supports identity revocation and cipher text 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.

References

[1]A. Shamir, “Identity-based cryptosystems and signature schemes,” in Advances in cryptology. Springer, 1985, pp. 47–53.

[2] D. Boneh and M. Franklin, “Identity-based encryption from the weil pairing,” SIAM Journal on Computing, vol. 32, no. 3, pp. 586–615, 2003.

[3]S. Micali, “Efficient certificate revocation,” Tech. Rep., 1996.

[4] W. Aiello, S. Lodha, and R. Ostrovsky, “Fast digital identity revocation,” in Advances in Cryptology–CRYPTO 1998. Springer, 1998, pp. 137–152.

[5]D. Naor, M. Naor, and J. Lotspiech, “Revocation and trac- ing schemes for stateless receivers,” in Advances in Cryptology– CRYPTO 2001. Springer, 2001, pp. 41–62.

[6]C. Gentry, “Certificate-based encryption and the certificate revo- cation problem,” in Advances in Cryptology–EUROCRYPT 2003. Springer, 2003, pp. 272–293.

[7]V. Goyal, "Certificate revocation using fine grained certificate space partitioning," in Financial Cryptography and Data Security. Springer, 2007, pp. 247–259.

[8]A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with efficient revocation," in Proceedings of the 15th ACM conference on Computer and communications security. ACM, 2008, pp. 417–426.

[9]B. Libert and D. Vergnaud, "Adaptive-id secure revocable identity- based encryption," in Topics in Cryptology–CT-RSA 2009. Springer,2009, pp. 1–15.

[10] "Towards black-box accountable authority ibe with short ciphertexts and private keys," in Public Key Cryptography–PKC 2009. Springer, 2009, pp. 235–255.

[11] K. Liang, J. K. Liu, D. S. Wong, and W. Susilo, "An efficient cloud- based revocable identity-based proxy re-encryption scheme for public clouds data sharing," in Computer Security-ESORICS 2014. Springer, 2014, pp. 257–272.

[12] D.-H. Phan, D. Pointcheval, S. F. Shahandashti, and M. Strefler, "Adaptive cca broadcast encryption with constant-size secret keys and ciphertexts," International journal of information security, vol. 12, no. 4, pp. 251–265, 2013.

[13] R. Anderson, "Two remarks on public-key cryptology (invited lecture)," 1997.

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

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

[16]A. Kozlov and L. Reyzin, "Forward-secure signatures with fast key update," in Security in communication Networks. Springer,

[17] 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.

[18] J. Yu, R. Hao, F. Kong, X. Cheng, J. Fan, and Y. Chen, "Forward- secure identity-based signature: security notions and construc- tion," Information Sciences, vol. 181, no. 3, pp. 648–660, 2011.

.