SECURE CLOUD DATA SHARING IN IDENTITY BASED CRYPTOGRAPHY USING REVOCATION

ELIGETI RITIKA
M. Tech Student, St. Martins Engineering College, Hyderabad, Telangana, India

Dr. R. CHINA APPALA NAIDU
Professor, Department of CSE, St. Martins Engineering College, Hyderabad, Telangana, India

G. KEERTHI REDDY
Asst. Professor, Department of IT, St. Martins Engineering College, Hyderabad, Telangana, India

ABSTRACT:

Cloud computing thereby brings many benefits for the users. But, a problem exists when a user wants to outsource the valuable information in cloud. Necessarily, it is important to put cryptographically augmented access control on such data. So, an encouraging cryptographically primitive is needed to build a realistic data sharing system, i.e., Identity-based encryption. The access control in this Identity-based encryption is not fixed. For the security purpose, a mechanism must be implemented where a user is removed from the system as soon as his/her authorization is terminated. Consequently, the user which is removed cannot access the shared data anymore. Identity-based encryption is a promising cryptographically primitive to build a practical data sharing system. However, access control is not static. That is, when some user's authorization is expired, there should be a mechanism that can remove him/her from the system. Consequently, the revoked user cannot access both the previously and subsequently shared data. To this end, we propose a notion called revocable-storage identity-based encryption (RS-IBE), which can provide the forward/backward security of cipher text by introducing the functionalities of user revocation and cipher text update simultaneously.

Keywords: *User Repudiation, Identity-based encryption (IBE), Cloud Computing, revocable storage.*

I. INTRODUCTION

Cloud computing enables outsourcing of data and provides enormous space for memory by which it presents the computational capacity massively. Cloud provides the most flexible way of storing the data, for example, programs, images etc. and accessing them in the easiest way over the Internet rather than storing in hardware components and retrieving that information from the computer. In cloud storage, data integrity is one of the main aspects. Cloud provides the easiest way of outsourcing the data. Obviously, the outsourcing gives rise to the data which is out of control of the user which leads to hesitation as the information may be valuable. This is the major security threat to the information that is stored in the cloud. Also the data in the cloud cannot be accessed by the user, if his/her authentication is terminated.

Cipher text-policy Attribute-based Encryption [2], which is regarded as one of the most suitable technologies for data access control in cloud storage systems as the access control policies are directly provided by the data owners. The compounded authority is responsible for the attribute management and key distribution. The authority can be taken as the admin office and library management of college or university which enrolls the students and provides the identity cards separately. The user with attributes only satisfying the access policy can decrypt the data. Since the access policy is defined

over the attributes. E.g., ―student AND faculty‖ attributes issued by administration with respect to details entered. But actually attributes vary dynamically. A user may get entitled with some new attributes or revoked some current attributes commonly called as attribute revocation problem. This technology allows for much more efficient computing by centralizing storage, memory, processing and bandwidth. Cloud computing is a comprehensive solution that delivers IT as a file. Else time period is expired then user cannot access this file. And one more condition is that, if OTP is wrong then user enters into revoke list .In this paper, extra mechanism provided for the secure data sharing in cloud computing.

2.1 CERTIFICATE-BASED ENCRYPTION:

A certificate, namely a signature acts not only as a certificate but also as a decryption key. A key holder needs both its secret key and an up-to-date certificate from its CA to decrypt a message. Certificate-based encryption combines the best aspects of identity based encryption and public key encryption. Certificate includes at least the name of a user and its public key. Often, the certificate authority includes a serial number as well as the certificate issue date and expiration date. if a user accidentally reveals its secret key or an attacker actively compromises it, the user may be requested for the revocation of its certificate. Futherly, the user's company may request revocation if the user leaves the company or changes position and is no longer entitled to use the key. If a certificate is revocable, then the third parties cannot relay on that certificate unless the CA distributes certificate status information indicating whether the certificate is currently valid.

2.2 IDENTITY BASED ENCRYPTION:

Identity Based Encryption (IBE) takes a effective approach to the problem of encryption key management. IBE can use any string as a public key, enabling data to be protected without the need for certificates. Protection is provided by a key server that controls the generation of private decryption keys. By separating authentication and authorization from private key generation through the key server, permissions to generate keys can be controlled dynamically on a granular policy driven basis, facilitating granular control over access to information in real time.

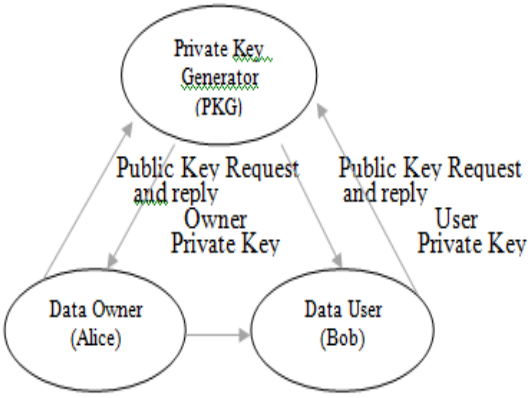

Fig 1: Identity based encryption

Identity-based systems allow any user to generate a public key from a known identity value such as an ASCII string. A trusted third party, called the Private Key Generator (PKG), generates the corresponding private keys. To operate, the PKG first publishes a master public key, and retains the corresponding master private key. Given the master public key, any user can compute a public key corresponding to the identity ID by combining the master public key with the identity value. To obtain a corresponding private key, the user authorized to use the

identity ID contacts the PKG, which uses the master private key to generate the private key for Identity ID. Thus, users may encrypt messages with no prior distribution of keys between individual participants. This is extremely useful in cases where pre-distribution of authenticated keys is inconvenient or infeasible due to technical restraints. However, to decrypt or sign messages, the authorized user must obtain the appropriate private key from the PKG.

2.3 IDENTITY BASED ENCRYPTION WITH EFFICIENT REVOCATION*:*

There is a security issue in IBE, to avoid it efficient revocation suggested that users renew their private period. Only the PKG's public key and the receiver's identity are needed to encrypt, and there is no way to communicate to the senders that an identity has been revoked, such a mechanism to regularly update users' private keys seems to be the only viable solution to the revocation problem. This means that all users, regardless of whether their keys have been exposed or not, should regularly get in contact with the PKG, prove their identity and get new private keys. The PKG must be online for all such transactions, and a secure channel must be established between the PKG and each user to transmit the private key. Taking scalability of IBE deployment into account, we observe that for a very large number of users this may become a bottleneck. We note that alternatively, to avoid the need for interaction and a secure channel, the PKG may encrypt the new keys of non-revoked users under their identities and the previous time period, and send the cipher texts to these users (or post them online). With this approach, for every non-revoked user in the system, the PKG is required to perform one key generation and one encryption operation per key update. We note that this solution, just as the original suggestion, requires the PKG to do work linear in the number of users, and does not scale well as the number of users grow.

2.4 REVOCABLE STORAGE IDENTITY BASED ENCRYPTION:

The non-revocable 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 process of decrypt-then-reencrypt 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. This process brings great communication and computation cost, and thus is cumbersome and undesirable for cloud users with low capacity of computation and storage.

III. CLOUD SECURITY

Besides, to overcome the above security threats, such kind of identity-based access control placed on the shared data should meet the following security goals: A. Data confidentiality: Unauthorized users should be prevented from accessing the plaintext of the shared data stored in the cloud server. In addition, the cloud server, which is supposed to be honest but curious, should also be deterred from knowing plaintext of the shared data. B. Backward secrecy: Backward secrecy means that,

when a user's authorization is expired, or a user's secret key is compromised, he/she should be prevented from accessing the plaintext of the subsequently shared data that are still encrypted under his/her identity. C. Forward secrecy: Forward secrecy means that, when a user's authority is expired, or a user's secret key is compromised, he/she should be prevented from accessing the plaintext of the shared data that can be previously accessed by him/her. The plaintext of the subsequently shared data that are still encrypted under his/her identity.

In Cipher text-Policy Attribute-Based Encryption [3] many situations exist, when a user encrypts sensitive data, it is imperative that she establish a specific access control policy on who can decrypt this data. For example, suppose that the FBI public corruption offices in Knoxville and San Francisco are investigating an allegation of bribery involving a San Francisco lobbyist and a Tennessee congressman. The head FBI agent may want to encrypt a sensitive memo so that only personnel that have certain credentials or at- tributes can access it. For instance, the head agent may specify the following access structure for access in this information: ((―Public Corruption Office ―AND (―Knoxville‖ OR ―San Francisco‖)) OR (management-level > 5) OR ―Name: CharlieEppes‖). By this, the head agent could mean that the memo should only be seen by agents who work at the public corruption offices at Knoxville or San Francisco, FBI officials very high up in the management chain, and a consultant named Charlie Eppes. As illustrated by this example, it can be crucial that the person in possession of the secret data be able to choose an access policy based on specific knowledge of the underlying data. Furthermore, this person may not know the exact identities of all other people who should be able to access the data, but rather she may only have a way to describe them in terms of descriptive attributes or credentials. Merits: We provide the first construction of a cipher text policy attribute-based encryption (CP-ABE) to address this problem, and give the first construction of such a scheme. In our system, a user's private key will be associated with an arbitrary number of attributes expressed as strings. On the other hand, when a party encrypts a message in our system, they specify an associated access structure over attributes. A user will only be able to decrypt a cipher text if that user's attributes pass through the cipher text's access structure. At a mathematical level, access structures in our system are described by a monotonic ―access tree‖, where nodes of the access structure are composed of threshold gates and the leaves describe attributes. Demerits: It would be interesting to consider attribute-based encryption systems with different types of expressibility. While, Key-Policy ABE and Cipher text-Policy ABE capture two interesting and complimentary types of systems there certainly exist other types of systems. The primary challenge in this line of work is to find new encrypted with a set of attributes for each authority, a user must have received from each authority policy which allows decryption for that set of attributes. Gopal et al. also presents large universe access structure scheme (an extension of the large universe scheme in SW). Demerits: One major limitation to the SW scheme. In their scheme, as in every IBE scheme, the user must go to a trusted party and prove his identity in

order to obtain a secret key which will allow him to decrypt messages.

IV. 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. In the traditional PKI setting, the problem of revocation has been well studied 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 first proposed a natural revocation way for IBE. They appended the current time to the cipher text, and non-revoked users periodically received private keys for each time 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. To conquer this problem, Boldyreva, Goyal and Kumar 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, Libert and Vergnaud proposed an adaptively secure RIBE scheme based on a variant of Water's IBE scheme, Chen et al. constructed a RIBE scheme from lattices. Recently, Seo and Emura proposed an efficient RIBE scheme resistant to a realistic threat called decryption key exposure, which means that the disclosure of decryption key for current time period has no effect on the security of decryption keys for other time periods. Inspired by the above work and Liang et al. Introduced a cloud-based revocable identity-based proxy re-encryption that supports user revocation and cipher text update. To reduce the complexity of revocation, they utilized a broadcast encryption scheme to encrypt the cipher text of the 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 resist the collusion of revoked users and malicious non-revoked users as malicious 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.

V. FORWARD-SECURE CRYPTOSYSTEMS

In 1997, Anderson [8] 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. 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 then transformed it into a forward-secure encryption with provable security in the random oracle model. Based on Canetti et al's approach, Yao et al. proposed a forward-secure hierarchical IBE by employing two hierarchical IBE schemes, and Nieto et al. designed a forward-secure hierarchical predicate encryption. Particularly, by combining Boldyreva et al.'s [12] revocation technique and the aforementioned idea of forward security1, in CRYPTO 2012 Sahai, Seyalioglu and Waters [7] proposed a generic construction of so-called revocable storage attribute-based encryption, which supports user revocation and cipher text update simultaneously. In other words, their construction provides both forward and backward secrecy. What must be pointed out is that the process of cipher text update of this construction only needs public information. However, their construction cannot be resistant to decryption key exposure, since the decryption is a matching result of private key and update key.

VI. PROPOSED METHODOLOGY

The proposed methodology of RIBE maintains the data integrity and also achieves the forward and backward secrecy. This also maintains the privacy of the users. This is because for the sharing of the data the data provider only considers the social information of the users. As this consideration doesn't require the private knowledge of the users, the identities of the users are safe. An RIBE dependent system of data sharing will work as follows:

Step 1: Firstly, the data provider (e.g., Dave) first determines the users (e.g., Bob and Alice) with whom the data can be shared. Using their identities, Dave encrypts and uploads this cipher text to the virtual server in the cloud for Bob and Alice.

Step 2: By downloading the cipher text and decrypting it, Bob as well as Alice can get the data that is shared. Nevertheless, for the unauthenticated user and the server, the data which is in the form of plaintext will not be available.

Step 3: In certain cases, e.g., when Bob's authorization is terminated, the shared data cipher text is downloaded by the data provider Dave. Dave will decrypt the cipher text and then re-encrypts the data so that Bob is forbidden from being able to access it and then the re-encrypted data is uploaded to the cloud once more. Now the user Bob is made available with the data. And the user can download the cipher text and by decrypting it, the plaintext will be made available.

Explicit interpretations are presented for RS-IBE and also its parallel security model. We present a specific architecture of RS-IBE. The confidentiality of the valuable information and backward/forward secrecy are implemented simultaneously by this proposal. By the presumption of the decisional ℓ Bilinear Diffie-Hellman Exponent (ℓ-BDHE), the secrecy of the proposed system in the defined model. Additionally, the proposed model can endure decryption key exposure. This not only achieves the integrity of the data but also the confidentiality.

VII. PERFORMANCE DISCUSSIONS

In this section, we discuss the performance of the proposed RS-IBE scheme by comparing it with previous works in terms of communication and storage cost, time complexity and functionalities, these schemes all utilize binary data structure to achieve revocation. Furthermore, by delegating the generation of re-encryption key to the key authority, the cipher text size of this system also achieves constant. At this end, the key authority has to maintain a data table for each user to store the user's secret key for all time periods.

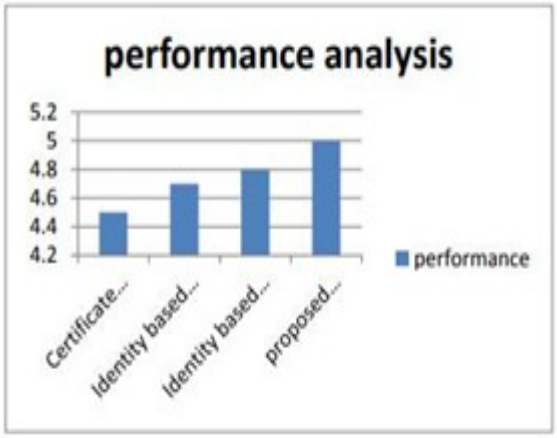

Fig 2: Identity based encryption

VIII. RESULT ANALYSIS AND DISCUSSIONS

The proposed scheme (Libert and Vergnaud, Seo and Emura, Liang et al) have same time complexity for encryption whereas the proposed system implements a efficient time complexity. The time complexity of decryption maintain constant in all the systems. The schema provides logarithmic storage of users identity instead of linear storage for user identity storage. As the time complexity decreases the number of users involved increases with no effect in performance of the system. Based on the sample data of the table is derived to explain the performance improvement in terms of time complexity.

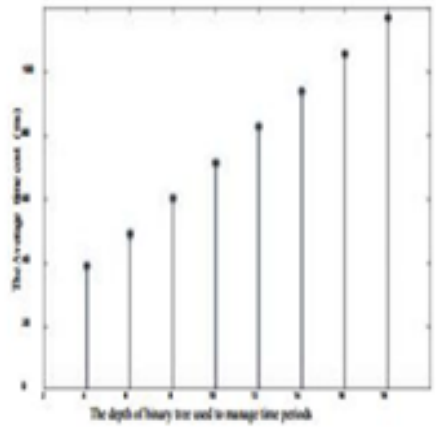

Fig 3: Encryption based on algorithm

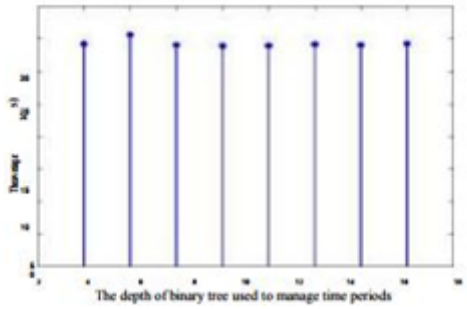

Fig 4: Decrypt

IX.CONCLUSION

Cloud computing has brought vast comfort for the society and the individuals. The increased need of allocating the data over the Internet is acquired by the Cloud. This paper we are introducing a new approach i.e. RS-IBE that particularly builds a data sharing system which is profitable and protective in cloud computing. RS-IBE prevents a repudiated user from accessing already shared data, as well as latterly shared data, representing identity revocation and cipher text update at the same time. Furthermore, a definite structure of RS-IBE is shown. Under the assumption of the decisional ℓ-DBHE, a flexible and security is evidently shown by the proposed established model of RS-IBE. After comparing the results, it is shown that the proposed RS-IBE has expediencies as per productivity and

operability. Hence the scheme is more viable foe realistic applications.

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. *M. Divya Sai , Dr.R.China Appala Naidu, Sudha Rani.V M.SaiKrishna Murthy and K.Meghana, " An Advanced Authentication system for multi server environment With Snort" International Conference on Advances in Computing, Communications and Informatics(ICACCI-2016), The LNM Institute of Information Technology, Jaipur, India, ISBN No.978-1- 5090-2028- 7, pp. 2527-2533, September 2016. (IEEE Explore, SCOPUS,DBLP)*
3. *ICloud. (2014) Apple storage service.[Online]. Available: https://www.icloud.com*
4. *R.China Appala Naidu, K. Meghana, P.S.Avadhani and I. Uma Maheswara rao, " New Approach of Authentication Method based on Profiles", Proceedings of the 2016 IEEE 3 rd International Conference on Recent Advances in Information Technology (RAIT-2016), Indian School of Mines(ISM), Dhanbad, Jharkhand, India, ISBN No. 978-1- 4799-8578-4, pp. 347-351, March 2016. (IEEE Explore, DBLP)*
5. *D. Boneh and M. Franklin, ―Identity-based encryption from the weil pairing,‖ SIAM Journal on Computing, vol. 32, no. 3, pp. 586– 615, 2003.*
6. *Anusha R and Dr.R.China Appala Naidu "Decentralized Access Control with policy hiding to store data in clouds" International Journal of software and Hardware Research in Engineering, ISSN:2347-4890, Volume 3, Issue 9, pp.20-25, September 2015.[Indexed in DRJI, SIS]*
7. *S. Micali, ―Efficient certificate revocation,‖ Tech. Rep., 1996.*
8. *E.Sowmya, Dr.R.China Appala Naidu, A.Santhoshi and A.S.V.R.R.Prasad" A Dynamic and Trust Based Privacy Preserving Mechanism to secure the data during transmission using cryptography" International Journal of Advanced Research in Computer and Communication Engineering, ISSN (online) :2278-1021, ISSN (print):2319-5940, Volume 4, Issue 10, pp.199-204, October 2015. [Indexed in Google Scholar, DRJI, Index Copernicus, OAJI]*
9. *B. Lynn. (2014) Pbc library: The pairing-based cryptography library. [Online]. Available: http://crypto.stanford.edu/pbc*
10. *Bhoga Ramya and Dr.R.China Appala Naidu "An Effective Secure Information Access model different Trusters" International Journal of Reviews on Recent Electronic & Computer Science (IJRRECS), ISSN 2321-5461Volume 4, Issue 8,June 2016 pp. 5921-5926, August 2016. [Indexed in Google Scholar, Slide Share]*
11. *M. Abdalla and L. Reyzin, ―A new forward-secure digital signature scheme,‖ in Advances in Cryptology– ASIACRYPT 2000. Springer, 2000, pp. 116–129.*
12. *Swathi Amancha, Dr. R.China Appala Naidu, Venkateswara Rao Bolla and K.Meghana, " Modern Approach of Detecting Packet Loss and Recovery in the Networks", Proceedings of the 2016 IEEE International Conference on Electrical,Electronics, and Optimization Techniques (ICEEOT)-2016, DMI College of Engineering, Chennai, Tamilnadu, India, ISBN No. 978-1-4673-9939- 5, March 2016. (IEEE Explore)*
13. *G. Anthes, ―Security in the cloud,‖ Communications of the ACM, vol. 53, no. 11, pp. 16–18, 2010.*
14. *Swetha sri and Dr.R.China Appala Naidu "Confidentiality Planning Implication Of User-Uploaded Images On Contented Distribution Sites" International Journal of Innovative Technology and Research (IJITR), ISSN 2320 –5547,Volume 4, Issue 6, pp. 5315-5317, Nov 2016. [Indexed in Google Scholar, Slide Share] R. Anderson, ―Two remarks on public-key cryptology (invited lecture),‖ 1997.*
15. *BANDARI SHRUTHI and Dr.R.China Appala Naidu "Right Key Conversation Protocols For Similar Network Categorizer Systems" International Journal of Innovative Technology and Research (IJITR), ISSN 2320 –5547,Volume 4, Issue 6, pp. 5312-5314, Nov 2016. [Indexed in Google Scholar, Slide Share]*