ENGINEERING IN ADVANCED RESEARCH SCIENCE AND TECHNOLOGY

ISSN 2350-0174
Vol.02, Issue.11
November -2020
Pages: -225-230

DATA SECURITY AND PRIVACY FOR GROUP DATA SHARING IN MULTIPLE DATA OWNERS AND ACCESSORS

[1]MOPURI PRIYANKA [2]KAMBHAM SALIVAHANA REDDY, M. tech (Assistant professor)

[1,2]Global College of Engineering and Technology, Department CSE

ABSTRACT: With the rapid development of cloud services, huge volume of data is shared via cloud confidentiality in cloud computing, current mechanisms cannot enforce privacy concerns over cipher text associated with multiple owners, which makes co-owners unable to appropriately control whether data disseminators can actually disseminate their data. In this paper, we propose a secure data group sharing and conditional dissemination scheme with multi-owner in cloud computing, in which data owner can share private data with a group of users via the cloud in a secure way, and data disseminator can disseminate the data to a new group of users if the attributes satisfy the access policies in the cipher text .We further present a multiparty computing. Although cryptographic techniques have been utilized to provide data access control mechanism over the disseminated cipher text, in which the data co-owners can append new access policies to the cipher text due to their privacy preferences. Moreover, three policy aggregation strategies, including full permit, owner priority and majority permit, are provided to solve the privacy conflicts problem caused by different access policies. The security analysis and experimental results show our scheme is practical and efficient for secure data sharing with multi-owner in cloud computing.

Keywords: Data sharing, cloud computing, conditional proxy re-encryption, attribute-based encryption, privacy conflict.

1 INTRODUCTION: The popularity of cloud computing is obtained from the benefits of rich storage resources and instant access [1]. It aggregates the resources of computing infrastructure, and then provides on-demand services over the Internet. Many famous companies are now providing public cloud services, such as Amazon, Google, Alibaba. These services allow individual users and enterprise users to upload data (e.g. photos, videos and documents) to cloud service provider (CSP), for the purpose of accessing the data at any time anywhere and sharing the data with others. In order to protect the privacy of users, most cloud services achieve access control by maintaining access control list (ACL). In this way, users can choose to either publish their data to anyone or grant access rights merely to their approved people. However, the security risks have raised concerns in people, due to the data is stored in plaintext form by the CSP. Once the data is posted to the CSP, it is out of the data owner's control [2]. Unfortunately, the CSP is usually a semi-trusted server which honestly follows the designated protocol, but might collect the users' data and even use them for benefits without users' consents. On the other hand, the data has tremendous usages by various data consumers to learn the behaviour of users [3]. These security issues motivate the effective solutions to protect data confidentiality. It is essential to adopt access control mechanisms to achieve secure data sharing in cloud computing [4]. Currently, cryptographic mechanisms such as attribute-based encryption (ABE) [5], identity-based broadcast encryption (IBBE) [6], and remote attestation [7] have been exploited to settle these security and privacy problems. ABE is one of the new cryptographic mechanisms used in cloud computing to reach secure and finegrained data sharing [8]. It features a mechanism that enables an access control over encrypted data using access policies and ascribed attributes among decryption keys and cipher texts. As long as the attribute set satisfies the access policy that the cipher text can be decrypted. IBBE is another prevalent technique employed in cloud computing [9, 10], in which users could share their encrypted data with multiple receivers at one time and the public key of the receiver can be regarded as any valid strings, such as unique identity and email. In fact, IBBE can be seen as a special case of ABE for policies consisting of an OR gate. Compared to ABE in which the secret key and cipher text are both correspond to a set of attributes, IBBE incurs low-cost key management and small constant policy sizes, which is more suitable for securely broadcasting data to specific receivers in cloud computing. Hence, by using identities, data owner can share data with a group of users in a secure and efficient manner, which motivates more users to share their private data via cloud. Actually, these encryption techniques can prevent unauthorized entities (e.g. semi-trusted CSP and malicious users) from accessing the data, but it may not consider data dissemination in cloud collaboration scenario such as Box [11] and One Drive [12], the data disseminators (e.g. editor and collaborator) may share the documents with new users even those outside the organization. However, once the data is encrypted with the above techniques, data disseminators are not able to modify the cipher text uploaded by data owners [13]. Proxy re-encryption (PRE) scheme [14] is employed to achieve secure data dissemination in cloud computing by delegating a re-encryption key associated with the new receivers to the CSP. However, the data disseminator can disseminate all of the data owner's data to others with this re-encryption key, which may not meet the practical requirement since the data owner may only permit the data disseminator to disseminate a particular document. A refined concept referred to as conditional PRE (CPRE) [15, 16] could address this issue, in which data owner can enforce re-encryption control over the initial cipher texts and only the cipher texts satisfying specific condition can be re-encrypted with corresponding encryption key. However, traditional CPRE schemes only support simple keyword conditions, so they cannot match complex situations in cloud computing well. In order to support expressive conditions rather than keywords, attribute-based CPRE is proposed [17], which deploys an access policy in the cipher text. The re-encryption key is associated with a set of attributes, thus the proxy can encrypt the cipher text only when the reencryption key matches the access policy. In this way, data owner can customize fine-grained dissemination condition for the shared data. Besides the requirement of conditional data dissemination, multiparty access control problem for data sharing in cloud computing such as cloud collaboration and cloud-based social networks comes along [18, 19], which means the special authorization requirements from multiple associated users can be accommodated together to control the shared data. Consider an example where a co-authoring document or a co-photo in cloud computing with three users, Alice, Bob, and Carol. If Alice who is the data owner uploads this co-authoring document or cophoto to the CSP and tags both Bob and Carol as the crowners. Alice can restrict this data to be disseminated to a certain group of users, while the coowners Bob and Carol may have different privacy concerns about this data. It is a massive and serious privacy problem if applying the preference of only one party, which may cause such data to be shared with undesired receivers. However, merging privacy preferences of data owner and multiple co-owners is not an easy task, due to privacy conflict is inevitable in multiparty authorization enforcement [20, 21]. Privacy conflict happens when the crowners have opposite privacy policies, and it results in data being impossibly accessed with anyone [22]. To deal with this dilemma, multiparty access control mechanisms'. (e.g. voting scheme) are further provided. However, all of them are based on plaintext data. In this paper, we propose an identity-based secure data group sharing and conditional dissemination scheme with multi-owner in cloud computing. To mitigate the problems mentioned above, we introduce a solution to achieve cipher text group sharing among multiple users, and capture the core feature of multiparty authorization requirements.

II. RELATED WORK

A. Shamir, "Identity-based cryptosystems and mark schemes [5]" The idea of identity-based encryption was presented by Shamir and advantageously instantiated by Boneh and Franklin. IBE wipes out the requirement for giving an open key framework (PKI). D. Boneh and M. Franklin, "Identity-based encryption from the Weil blending [6]" There ought to be a way to deal with deny clients from the framework when essential, e.g., the expert of some client is terminated or the secret key of some client is unveiled. In the conventional PKI setting, the issue of disavowal has been very much examined by S. Micali, W. Aiello, S. Lodha, and R. Ostrovsky, D. Naor, M. Naor, and J. Lotspiech, C. Nobility, V. Goyal, and a few methods are generally affirmed, for example, certi_cate renouncement list or adding legitimacy periods to declarations. In any case, there are just a couple of concentrates on renouncement in the setting of IBE. Boneh and Franklin proposed a characteristic denial path for IBE. They affixed the present timeframe to the ciphertext, and nonrepudiated clients occasionally got private keys for each timespan from the key expert. Lamentably, such an answer isn't versatile, since it requires the key specialist to perform direct work in the quantity of non-renounced clients. What's more, a safe channel is basic for the key specialist and non-renounced clients to transmit new keys. A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with e_cient repudiation "[7][8] To overcome this issue, Boldyreva, Goyal, and Kumar acquainted a novel methodology with accomplish proficient denial. They utilized a parallel tree to oversee identity with the end goal that their RIBE plan decreases the multifaceted nature of key disavowal to logarithmic (rather than straight) in the most extreme number of framework clients. In any case, this plan just accomplishes particular security. B. Libert and D. Vergnaud, "Versatile id secure revocable identity-based encryption "[9] The creator proposed an adaptively secure RIBE plan based on a variation of Water's IBE plot, Chen et al. developed a RIBE plot from grids. J. H. Web optimization and K. Emura, "Revocable identity-based encryption returned to: Security model and construction"[10] Recently, Seo and Emura proposed a productive RIBE conspire impervious to a reasonable danger called decoding key presentation, which implies that the divulgence of unscrambling key for current timeframe has no impact on the security of decoding keys for other timespans. 6. K. Liang, J. K. Liu, D. S. Wong, and W. Susilo, "A proficient cloud-based revocable identity-based intermediary re-encryption conspire for open clouds data sharing". Motivated by the work Liang presented a cloud-based revocable identity-based intermediary re-encryption that supports client denial and ciphertext update. To lessen the multifaceted nature of renouncement, they used a communicate encryption plan to scramble the ciphertext of the update key, which is autonomous of clients, with the end goal that solitary no repudiated clients can decode the update key. In any case, this sort of renouncement technique can't avoid the plot of disavowed clients and malevolent non-denied clients as pernicious non-repudiated clients can share the update key with those denied clients. Moreover, to refresh the ciphertext, the key specialist in their plan needs to keep up a table for every client to create the reencryption key for each timespan, which fundamentally builds the key expert s outstanding burden.

III. Methodology

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.

Key Revocation Process Revocation means recall. By public key infrastructure and Certificate Revocation List (CRL) therevocation 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

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 an 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:

Conclusion:

The data security and privacy is a concern for users in cloud computing. In particular, how to enforce privacy concerns of multiple owners and protect the data confidentiality becomes a challenge. In this, we present a secure data group sharing and conditional dissemination scheme with multi-owner in cloud computing. In our scheme, the data owner could encrypt her or his private data and share it with a group of data accessors at one time in a convenient way based on IBBE technique. Meanwhile, the data owner can specify fine-grained access policy to the cipher text based on attribute-based CPRE, thus the cipher text can only be re-encrypted by Data disseminator whose attributes satisfy the access policy in the cipher text. We further present a multiparty access control mechanism over the cipher text, which allows the data co-owners to append their access policies to the cipher text. Besides, we provide three policy aggregation strategies including full permit, owner priority and majority permit to solve the problem of privacy conflicts.

Future work

In the future, we will enhance our scheme by supporting keyword search over the ciphertext.

References [1]. L. M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, "A break in the clouds: towards a cloud de_nition" ACM SIGCOMM Computer Communication Review, vol. 39, no. 1, pp. 50 55, 2008. [2]. 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. [3]. 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. [4]. G. Anthes, Security in the cloud, Communications of the ACM, vol. 53, no. 11, pp. 16 18, 2010. [5]. A. Shamir, Identity-based cryptosystems, and signature schemes, in Advances in cryptology. Springer, 1985, pp. 47 53. [6]. D. Boneh and M. Franklin, Identity-based encryption from the Weil pairing, SIAM Journal on Computing, vol. 32, no. 3, pp. 586 615, 2003. [7]. V. Goyal, Certi_cate revocation using _ne grained certi_cate 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 e_cient 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]. J. H. Seo and K. Emura, Revocable identity-based encryption revisited: Security model and construction, in Public-Key Cryptography PKC 2013. Springer, 2013, pp. 216 234.