International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 01, January-2020

Survey on Block Design-based Key Agreement for Group Data Sharing in Cloud Computing

Dr. M. Ramesh Kumar[1], Sivagurunathan. A[2], Thukkaiprasanth. T[3], UdhayaKumar. C[4], Vignesh.R. S[5]
Department of Computer Science and Engineering
VSB College of Engineering Technical Campus Kinathukadavu, Coimbatore

***Abstract*:- The genuine purposes of this strategy a safe multi-proprietor data sharing arrangement. It derives that any customer in the social affair can securely give data to others by the untrusted cloud. This arrangement can support dynamic social occasions. Profitably, especially, new permitted customers can clearly unscramble data archives exchanged before their backing without coming to with data proprietors. Customer revocation can be successfully proficient through a novel foreswearing list without updating the puzzle Keys of whatever remains of the customers. The size and count overhead of encryption are steady and Independent with the amount of revoked customers. We present a safe and security ensuring access control to customers, which guarantee any part in a social event to anonymously utilize the cloud resource. Likewise, the veritable identities of data proprietors can be revealed by the get-together executive when open deliberation happen. We give careful security examination, and perform expansive generations to show the adequacy of our arrangement to the extent limit and estimation overhead. Disseminated figuring gives a traditionalist and gainful response for sharing social event resource among cloud customers. Shockingly, sharing data in a multi- proprietor way while shielding data and identity security from an untrusted cloud is still a testing issue, in light of the constant change of the enlistment.**

Keywords: Data sharing, cloud computing, advanced encryption standard, 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 behavior of users.

2. RELATED WORK

A series of unaddressed security and privacy issues emerge as important research topics in cloud computing. To deal with these threats, appropriate encryption techniques should be utilized to guarantee data confidentiality. By utilizing the IBBE technique [23], Huang et al. Patranabis et al.
[25] and Liu et al. proposed several private data sharing schemes in cloud computing. In these schemes, data owner outsources encrypted data to the CSP by defining a list of receivers, thus only the intended users in the list can get the decryption key and further decrypt the private data. ABE is another promising one-to-many cryptographic technique to realize data encryption and fine-grained access control in cloud computing [26, 27]. Specially, ciphertext-policy ABE (CP-ABE) is suited for access control in real world applications due to its expressiveness in describing the access policy of ciphertext [28]. Guo et al.
[29] proposed a privacy preserving data dissemination scheme in mobile social networks based on CP-ABE. Teng et al. [30] proposed an efficient access control scheme with hierarchical CP-ABE to achieve privacy preservation in cloud storage systems. In the schemes of [31] and [32], ABE has been utilized to provide access control of medical documents when providing health services in cloud, so that health record can only be decrypted by authorized document requesters with corresponding attributes. Secure data dissemination is another important security requirement for data storage in cloud computing. The identity-based PRE [33] is a basic encryption algorithm to reach secure data dissemination in cloud computing, with which the data disseminators could send their reencryption keys to the semi-trusted proxy to transform data owner's ciphertext for new users [34]. Further, attribute-based PRE [17] has been employed in cloud computing by incorporating the ABE technique. The proxy can transform the ciphertext under an access policy into the one under another access policy with data disseminator's re-encryption key, and the users who satisfy the new access policy can access the plaintext. However, the above PRE schemes only allow data dissemination in an all-ornone manner. This issue is further addressed by CPRE scheme [35], in which the proxy can successfully reencrypt the

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 01, January-2020

ciphertext only if the prescribed conditions are met. However, in earlier CPRE schemes [35, 36], the conditions are keywords only, which would limit the flexibility when enforcing complex delegations in cloud computing. Yang et al. [37] proposed an attribute-based CPRE scheme by deploying an access policy in a ciphertext generated by public-key encryption. The reencryption key is generated by the secret key associated with a set of attributes, which allows the proxy to re encrypt the ciphertext only when these attributes satisfy the access policy.
Wangetal. [38] proposed a preauthentication approach for sharing data in cloud, which achievereceiver attribute authentication before the encryption operation.

3. EXISTING SYSTEM:

Several security schemes for data sharing on untrusted servers have been proposed. In these approaches, data owners store the encrypted data files in untrusted storage and distribute the corresponding decryption keys only to authorized users. Thus, unauthorized users as well as storage servers cannot learn the content of the data files because they have no knowledge of the decryption keys However, the complexities of user participation and revocation in these schemes are linearly increasing with the number of data owners and the number of revoked users, respectively. By setting a group with a single attribute, Lu et al. proposed a secure provenance scheme based on the cipher text-policy attribute-based encryption technique, which allows any member in a group to share data with others. However, the issue of user revocation is not addressed in their scheme. presented a scalable and fine-grained data access control scheme in cloud computing based on the key policy attribute-based encryption (KP-ABE) technique. Unfortunately, the single owner manner hinders the adoption of their scheme into the case where any user is granted to store and share data.

Disadvantages:

It does not provide security for sharing the data within the groups. It does not provide privacy preserving access control to the users**.**

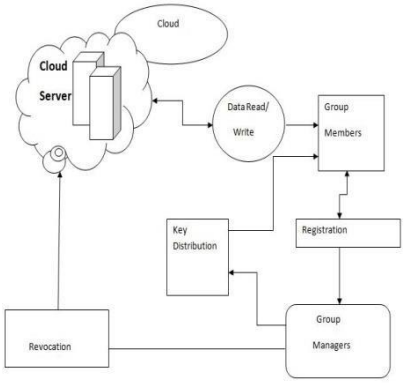
4. PROPOSED SYSTEM:

This paper, we propose a secure multiowner data sharing scheme, named Mona, for dynamic groups in the cloud. By leveraging group signature and dynamic broadcast encryption techniques, any cloud user can anonymously share data with others. Meanwhile, the storage overhead and encryption computation cost of our scheme are independent with the number of revoked users. In addition, we analyze the security of our scheme with rigorous proofs, and demonstrate the efficiency of our scheme in experiments.

ADVANTAGES:

We propose a secure multi-owner data sharing scheme. It implies that any user in the group can securely share data with others by the untrusted cloud. We provide secure and privacy-preserving access control to users, which guarantees any member in a group to anonymously utilize the cloud resource.

5. SYSTEM ARCHITECTURE:



6. HARDWARESPECIFICATION

- Main Processor : 2GHz
- Ram (min) : 512 MB
- Hard Disk : 80 GB

7. SOFTWARE SPECIFICATION

- Language : Java
- Web Server : Tomcat 6
- Operating System : Windows 7 32 Bit
- CloudSim

8. Development Report Front End Design:

- Html
- Css
- Js
- Jquery
- Bootstrap
- Ajax
- Jsp

Server Side Script:

- Servlet
- Core Java

Back End :

- MySQL

Technical Terms

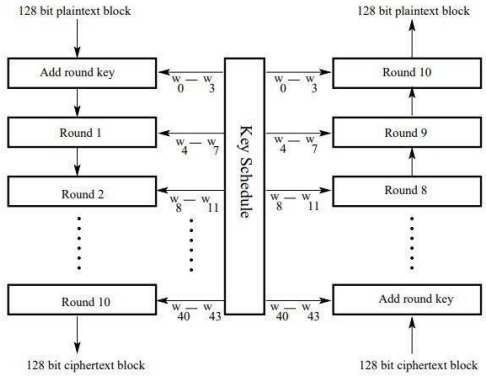
AES - Advanced Encryption Standard

9. AES:

AES is a block cipher with a block length of 128 bits. It allows for three different key lengths: 128, 192, or 256 bits. Most of our discussion will assume that the key length is 128 bits. Encryption consists of 10 rounds of

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 01, January-2020

processing for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys. Except for the last round in each case, all other rounds are identical. To appreciate the processing steps used in a single round, it is best to think of a 128-bit block as consisting of a 4 × 4 array of bytes, arranged as follows. Whereas AES requires the block size to be 128 bits, the original Rijndael cipher works with any block size (and any key size) that is a multiple of 32 as long as it exceeds 128. The state array for the different block sizes still has only four rows in the Rijndael cipher. However, the number of columns depends on size of the block. For example, when the block size is 192, the Rijndael cipher requires a state array to consist of 4 rows and 6 columns.



10 .PERFORMANCE ANALYSIS:

We next analyze the performance of our scheme. Generally, the costs of pairing and exponentiation operations dominate the major computation time, thus we ignore the multiplication, hash, symmetric encryption and decryption computation. Let Nc be the number of attributes in

TABLE 3
COMPUTATION EFFICIENCY

Phase		Computation cost
Key generation		$(2\|S\|+3)T_{exp0}$
Data encryption	Full permit	$2T_{exp1}+(2\|U\|+2N_c+\|W\|+8)T_{exp0}$
	Owner priority	$2T_{exp1}+(3\|U\|+2N_c+\|W\|+12)T_{exp0}$
	Majority permit	$2T_{exp1}+(2\|U\|+2N_c\|W\|+4\|W\|+6)T_{exp0}$
Co-owner key generation		$T_{exp1}+(2N_c+5)T_{exp0}+2T_{pair}$
Policy appending	Full permit	$3T_{exp0}$
	Owner priority	$3T_{exp0}$
	Majority permit	0
Re-encryption key generation		$T_{exp1}+(\|U'\|+5)T_{exp0}$
Data re-encryption	Full permit	$(N_c+1)T_{exp1}+(\|U\|+3)T_{exp0}+(2N_c+4)T_{pair}$
	Owner priority	$T_0: (N_c+1)T_{exp1}+(\|U\|+2)T_{exp0}+(2N_c+4)T_{pair}$ $T_i: (N_c+1)T_{exp1}+(\|U\|+3)T_{exp0}+(2N_c+4)T_{pair}$
	Majority permit	$(N_c+t+1)T_{exp1}+(\|U\|+3)T_{exp0}+(2N_c+5)T_{pair}$
Data decryption	Initial or renewed ciphertext	$T_{exp1}+(\|U\|+2)T_{exp0}+2T_{pair}$
	Re-encrypted ciphertext	$T_{exp1}+(\|U'\|+2)T_{exp0}+3T_{pair}$

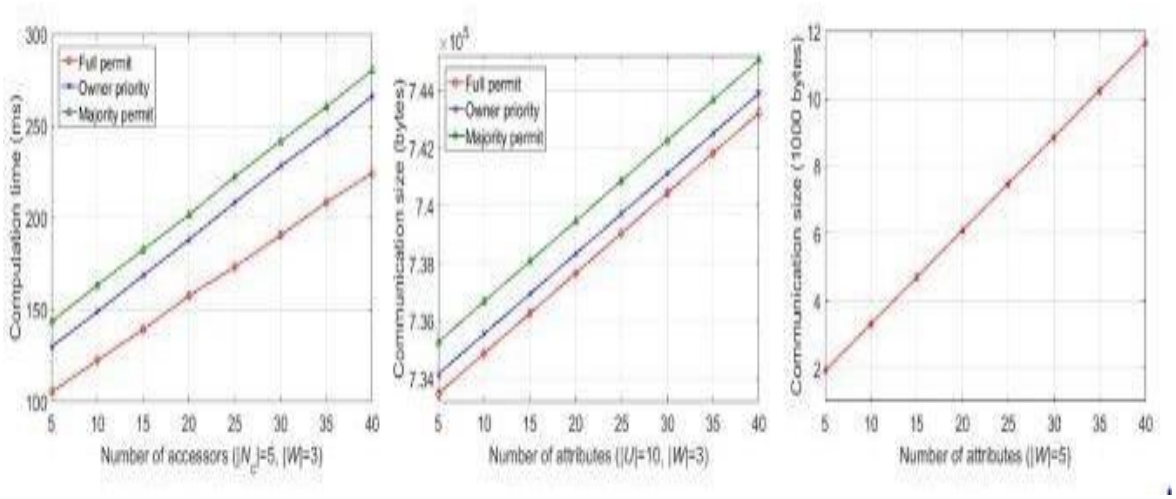
access policy, Tpair be the computation cost of a single pairing operation, Texp0 and Texp1 be the computation cost of an exponent operation on G0 and GT . Table 3 shows the computation cost of each phase in our scheme.First, data owner can choose one of three policy aggregation strategies to encrypt the data. The initial ciphertext is associated with an empty policy * T1 and
|W| number of empty policies * T1 in strategies of owner priority and majority permit respectively. Thus, the corresponding computation cost are 2Texp1+(3|U|+2Nc+|W|+12)Texp0 and2Texp1+(2|U|+2Nc|W|+4|W|+6)Texp0 in these two strategies which are more than that in full permit strategy.Then, data co-owners can renew the ciphertext by appending their access policies as the dissemination conditions into empty policy.

The computation cost in full permit and owner priority strategies are both 3Texp0, while the computation cost in majority permit strategy is onlythree multiplications. When the data disseminator dis-seminates a ciphertext to other users, he must send the reencryption key to the CSP. The CSP can re-encrypt ciphertext if he satisfies enough access policies in the ciphertext. According to different strategies adopted bydata owner, the CSP spends different computation cost.In owner priority strategy, the data disseminator must satisfy either T0 customized by data owner or Ti customized by all the data co-owners, of which the computation cost are (Nc+1)Texp1+(|U|+2)Texp0+(2Nc+4)Tpair and(Nc+1) Texp1+(|U|+3)Texp0+(2Nc+4) Tpair. In majority permit strategy, the CSP would spend(Nc+t+1)Texp1+(|U|+3)Texp0+(2Nc5) Tpair to re-encrypt ciphertext if data disseminatorsatisfies at least t access policy trees.Finally, data accessor can decrypt initial or renewed ciphertext with her or his private key SK if he is an intended receiver.

11. 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 paper, 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 this private data and share it with a group of data assessors at one time in a convenient

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 01, January-2020



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.

12.REFERENCES:

[1] L. Xu, C. Jiang, N. He, Z. Han, and A. Benslimane, "Trust-based col- laborative privacy management in online social networks," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 1, pp. 48- 60, 2019.

[2] H. Cui, X. Yi, and S. Nepal, "Achieving scalable access control over encrypted data for edge computing networks," *IEEE Access*, vol. 6, pp. 30049–30059, 2018.

[3] K. Xue, W. Chen, W. Li, J. Hong, and P. Hong, "Combining data owner-side and cloud-side access control for encrypted cloud storage," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 8, pp. 2062–2074, 2018.

[4] Q. Huang, Y. Yang, and J. Fu, "Secure data group sharing and dis- semination with attribute and time conditions in Public Clouds," *IEEE Transactions on Services Computing*,2018.

[5] J. M. Such and N. Criado, "Resolving multi-party privacy conflicts in social media," *IEEE Trans. on Knowledge and Data Engine*, vol. 28, no. 7, pp. 1851-1863,2016.

[6] K. Seol, Y. Kim, E. Lee, Y. Seo, and D. Baik, "Privacy-preserving at- tribute-based access control model for XML-based electronic health record system," *IEEE Access*, vol. 6, pp. 9114-9128, 2018.