ISSN: 2366-1313

MULTI-OWNER BASED PRIVACY ENABLED GROUP DATA SHARING IN CLOUD COMPUTING

[1]Dr. K.G.S VENKATESAN, [2]S AKHILA

[1]Assistant Professor, Dept. of CSE, Megha Institute of Engineering and Technology for Women,
venkatesh.kgs@gmail.com

[2]Assistant Professor, Dept. of CSE, Megha Institute of Engineering and Technology for Women,
akhila566@gmail.com

Abstract: *With the rapid improvement of cloud services, many statistics are shared through cloud computing. Although cryptographic techniques have been used to provide data privacy in cloud computing, the current methodology cannot enforce privacy concerns regarding ciphertext associated with multiple owners, allowing the participating owners to correctly unable to manipulate whether file disclosures can reveal their statistics. This paper proposes a conditional distribution and secure information sharing scheme with multiple owners in cloud computing. The owner of statistics can securely share personal data with a set of users through the cloud. Easy and record-releasing information can spread. Data to a new user organization if attributes fulfil the right of access to rules in the ciphertext. In addition, we've introduced a multiparty access mechanism for managing spread ciphertext, where data owners can add new ciphertext access policies due to their privacy choices. In addition, three strategies for collecting coverage: full consent, owner preference, and majority consent, are provided to resolve privacy disputes due to specific access laws. Security Analysis and Experimental Impacts show that our scheme to share comfortable data with multiple owners in cloud computing is sensible and environmentally friendly.*

Keywords: *Cloud computing, Data security, cryptographic techniques, Security Analysis*.

I. INTRODUCTION

More and more organizations and businesses are using cloud servers as their device platform in cloud computing. Today, the position-based version of full access to manipulation (RBAC) is the most popular model used in agency structures. However, this version has serious security issues when deployed in the cloud system. A traditional RBAC model uses reference monitors running on fact servers to enforce permissions. However, cloud servers are beyond the control of the organization's domains and should therefore be considered unreliable

ISSN: 2366-1313

by default. Therefore, creating an effective data protection mechanism for cloud-based business structures has become a major challenge.

Currently, encryption is the number one method used in the cloud to ensure data security. The Cloud Security Alliance (CSA) [1] suggests that an unusual technique for enhancing information security is to keep the information confidential, both in transit and when stored in the cloud. Although traditional encryption schemes, including Public Key Encryption and Identity based Encryption (IBE) [2], can ensure the confidentiality of data, they cannot be effectively implemented to manage them. However, privacy and access controls using data will be enforced if encrypted information acts as a right of access to the policy and can allow or deny clients primarily based on access to the policy. It can be done Instead of relying on unreliable cloud servers. This type of protection model, called autonomous data protection in this document, reduces reliance on cloud servers and prevents access and tampering with unauthorized files at any point of transmission. Therefore, independent data security primarily gives registries the ability to ensure their security and is a powerful mechanism for protecting data in the cloud. However, neither the RBAC itself nor the classical public encryption or perhaps a combination of both strategies [3] can meet the requirements of independent data protection.

That encryption technique may prevent unauthorized entities (such as semi-dependent CSPs and malicious clients) from accessing the data. Still, you may not notice the spread of data in cloud computing. In a cloud collaboration scenario that includes Box and OneDrive, Data Disclosure (for example, Publisher and Contributor) can share files with new customers, even those outside the company. However, after encrypting the data using the above techniques, statistic spreaders cannot edit the ciphertext uploaded by the record owners. The proxy re-encryption (PRE) scheme has been contracted to give CSP the benefit of easy information transmission in cloud computing by assigning a re-encryption key attached to the new receivers. However, with this re-encryption key, Data Disclosure can disclose all data owner's records to others, which may not meet the practical requirement since the data owner transmits a specific record to Data Disclosure. A better concept called conditional PRE (CPRE) should address this issue. The data owner can impose encryption manipulation on the initial ciphertexts and only the specific pleasing condition of the

ISSN: 2366-1313

ciphertexts. May return Encrypt with the relevant encryption key. However, traditional ERCP schemes only support simple keyword terms, so they do not adapt well to complex cloud computing conditions. To help with expressive situations rather than keywords, attribution-based CPRE is proposed, which implements policy access within ciphertext. The re-encryption key is associated with a set of attributes, so the proxy can only encrypt the ciphertext when the re-encryption key is suitable for access to coverage. The data owner can customize the first-class broadcast situation for shared records. For example, the records owner allows the company's business managers to post a record of progress on OneDrive. In contrast, only government administrators can use postwork budgets on OneDrive for a specified period in the finance branch.

II. RELATED WORK

In cloud computing, unspoken security and privacy issues become a major topic of study. To deal with these threats, appropriate encryption techniques must be applied to ensure the confidentiality of the data.

Patranabis et al [4]. They proposed several private data exchange schemes in cloud computing. In these schemes, the data owner outsources the encrypted data to the CSP by specifying a list of recipients. Only the desired users in the list can obtain the decryption key and decrypt the private data. ABE Cloud Computing has many secret ways to gain the right to data encryption and granular access. In particular, the ciphertext policy ABE (CP-ABE) is appropriate for accessing controls in real-world applications because of its expression in describing the ciphertext access policy.

Guo et al. [5] Recommendation for CP-ABE based privacy networks. It is an effective way to access the classified CP-ABE manipulation scheme to maintain confidentiality in cloud storage systems. ABE has been implemented in the schemes to provide access to medical documents while providing health services in the cloud. The applicant of the legal document can easily understand the health report with relevant attributes. Some research has focused on linking RBAC with various encryption schemes to protect data.

Crampton et al. [6] This introduced a new feature of the RBAC regulations, specifically the use of a partial sequence relation to describe policies. This technique translates RBAC policies into record float guidelines. Then, use the cryptographic application of the rules to create a cryptographic RBAC mechanism.

ISSN: 2366-1313

Zhu et al.[7] They proposed a cryptographic RBAC model with a function key classification (RKH) model that could guide function classification. In RKH, each set corresponds to a unique role key, and users are assigned a unique user key for each of their roles. However, because clients must retain a private key for each role, this approach will increase the key administrative burden, especially when multiple roles are assigned to the user. RBAC can also be combined with ABE to protect data in cloud computing.

Zhu et al. [8] It proposed ABE, according to RBAC, move the RBAC system primarily to ABE-based data security. Each character maps one or more attributes based on the migration proxy in this scheme. Then provided, an ABE scheme with attribute classification to encrypt the record with mapped attributes.

Zhou et al. [9] It proposed a complete role-based encryption (RBE) scheme that combined RBAC with CP-ABE for easy cloud storage. In RBE, data is encrypted using the role's public parameters, and users assigned to this role can decrypt the ciphertext. However, the RBE function cannot support inheritance. In the cryptographic version of the entry position for manipulation implemented by CP-ABE, each position is associated with the entry into the tree. Users whose attributes meet the function coverage tree may be allowed decryption. The scheme can handle dynamic principles, including permissions, role project changes, and document updates. However, this requires all actions from the owner of the information, which is unreasonable and unrealistic in the context of cloud computing.

Some approaches [9] they are proposed primarily based on a linear secret share scheme (LSSS). The expressive power of LSS is almost equal to the shape of a tree, except that every feature in the LSS structure can be used more easily. Some schemes have also been proposed which help the border operator more effectively. The AND operator is a limit (n, n); As a result, those schemes can also help the AND operator. In addition to AND, OR, and threshold operators, there are other complex operators, such as NOT and contrast operators (i.e.,>, ≥, <, and ≤), that may be most useful in practice but cannot.

III. PROPOSED WORK

This paper recommends an identity-based secure data sharing and conditional distribution scheme with multiple owners in cloud computing. To alleviate these problems, we offer a technique to achieve the institutional exchange of ciphertext between a couple of users and to get the

ISSN: 2366-1313

basic features of the multilateral authorization requirements.

The contributions of our scheme are as follows

(1) We achieve fine-grained conditioning dissemination on ciphertext in cloud computing with attribution based CPRE. The ciphertext is implemented first, with initial access to the custom policy by the data owner. Our proposed multilateral access to system management allows co-owners of statistics to add new ciphertext access policies as an alternative to their privacy. Therefore, the data spreader can re-encrypt the ciphertext if the attributes meet sufficient access principles.

(2) We offer three techniques for resolving privacy disputes: full consent, owner preference, and majority consent. Specifically, in a fully authorized approach, the data distributor must meet all entry requirements by the standards set by the data owner and co-owners. With a majority authorization procedure, the record owner can choose a threshold value for the co-owners of the first record, and ciphertext can be spread if the data is a combination of access to the rules. The disseminator attributes are high exceeding or equal to this limit.

(Iii) We demonstrate the accuracy of our scheme and practice experiences to evaluate the performance at each stage to identify the effectiveness of our scheme.

SYSTEM ARCHITECTURE

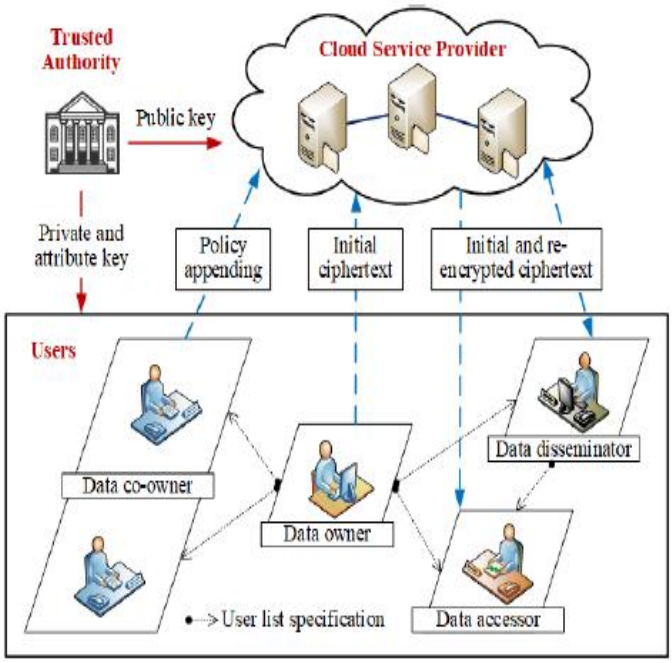

Fig.1 Proposed architecture

The system model consists of the following entities, as shown in Fig. 1. The notations used throughout this paper are presented in Table 1.

1) Trusted authority: The Trust Authority is a fully-fledged party that initiates the public key of the system and develops private keys and feature keys for the users. For example, this could be done through a corporation administrator or social security administration.

2) CSP: CSP is a semi-independent element that provides every user with a convenient record storage provider with

ISSN: 2366-1313

digital space and cloud infrastructure. It also includes policy access to cipher texts for data co-owners and develops encrypted cipher texts for clients.

3) User: We divide the individual's role into the following categories: record holder, statistic co-owner, statistician, and data accessor. The statistics owner can choose a way to collect the coverage and create an admissions policy to implement the broadcast scenarios. It then encrypts logs for a set of recipients and outsources ciphertext to CSPs for sharing and broadcasting. Co-owners of information tagged by the data owner can add access to CSP-encrypted data guidelines and generate the updated ciphertext. The data spreader can access the data and re-encrypt the key to pass the data owner's data to others if it complies with adequate access policies within the ciphertext. The data user can decrypt the initial, refreshed, and re-encrypted ciphertext with their private key.

Security Definitions and Goals

First, we expect that other entities will rely entirely on authority and will no longer be affiliated with any entity that also operates with the help of related functions. Therefore, we assume that CSP is semi-dependent; in fact, it may be as interesting as possible to perform entity requests and examine as many records as possible about the stored data. Furthermore, we trust the owners of records. However, some users will try to access data outside their privileges, including collaboration with other users and CSPs. Also, we no longer remember information model management, which means that once ciphertext is renewed, users cannot retrieve old ciphertext. We hope that using the management scheme, and Data ownership can be guaranteed. Cipher Text Deadplication [45]. In particular, the desire for safety can be summarized in observation.

1) Data confidentiality: Information should be included well against semi-dependent CSPs and unauthorized clients. Users who are not recipients of the cipher text described by the owner of the information or the revealer of the facts will no longer be able to access the plain text.

2) Fine-grained dissemination conditions: Data holders and data co-owners can customize high-grade granular and tree-based broadcast scenarios for their data. Cipher Text may only be distributed to users who meet these requirements.

3) Continuous policy enforcement: The data owner’s access policy is enforced in

ISSN: 2366-1313

the initial ciphertext as well as the renewed ciphertext.

4) Collusion resistance: If all the attributes of the data disclosure do not, in my opinion, meet the principles of access to cipher text with their attributes, then those users will not be able to combine and crack that cipher text.

IV. EXPERMENTAL RESULTS

In this segment, we apply our scheme to a crypto library paired with a 2.53 GHz Intel Core 2 Duo CPU and 4 GB of memory on a cloud server. A set of 160-bit type curves based on a well-matched elliptical curve y2 = x3 + x is used on a finite 512-bit field, and the general public parameters are selected to provide an 80-bit protection phase. We conducted several experiments and opted for the Advanced Encryption Standard (AES) because of the compatible encryption scheme. Experimental results are the implication of hundreds of trials. In the encryption phase, the statistics owner defines a set of identities, accesses the coverage, and then uploads the encrypted data to the CSP. We use computing time and communication size because of metric complexity. The calculation time is mainly linked to two factors: the number of people accessed and the characteristics of the policy entry. Figure 2 shows the calculation time of data encryption versus access to a faster and tougher policy with five features and three co-owners. Due to the facts, the owner will have to install one or more blank policies for the owners participating in the owner preference procedure and majority authorization procedure. More, Figure 3 compares the record owner's verbal exchange rate by choosing each of the 3 strategies. In general, ciphertext sizes grow linearly with Nc in three strategies. More specifically, the release price of the majority authorization strategy is the highest, and the release cost of the owner's preferred strategy is slightly higher than from the point of view of full authorization, as the owner has C7, C8, C9, and C10. The number of holdings is doubled in a preferred way. In the majority authorization strategy, the number of shares equals the number of co-owners, Figure 2 in 3.

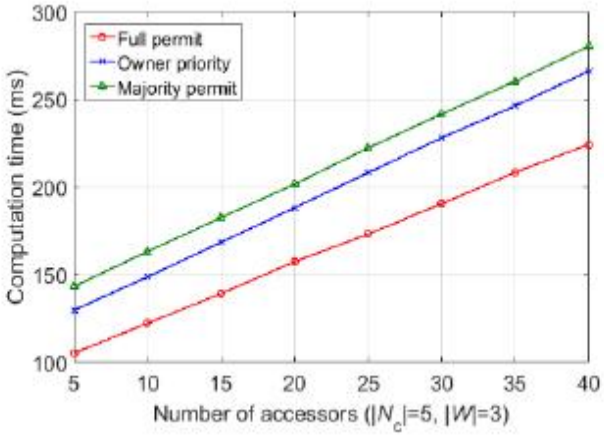

Fig. 2. Computation time versus users in encryption phase

ISSN: 2366-1313

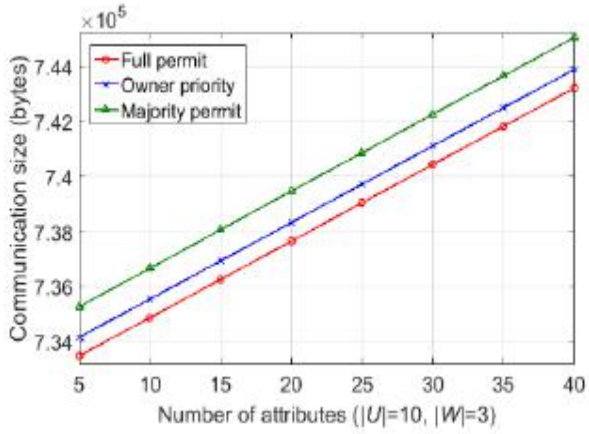

Fig.3 Communication size versus attributes in encryption phase

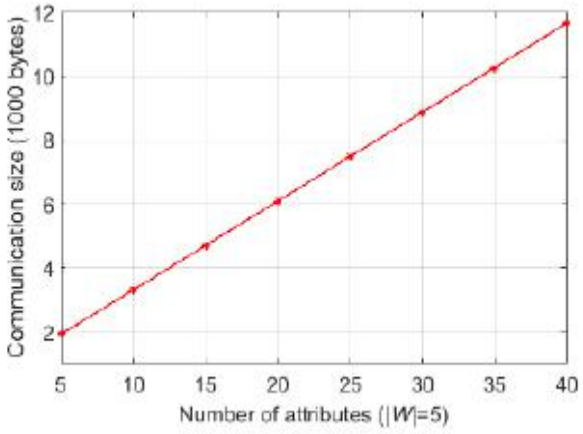

Fig.4 Communication size versus attributes in co-owner key generation phase

Experimental results show that encrypting shared information takes approximately 122 ms with 10 accessors during the full permissions procedure. The ciphertext length is optimal at 4145 bytes, whereas The number of attributes is 10. In the incremental phase of coverage, the communication cost for the co-owner of information is 3303 bytes, mainly due to the change key. The maximum calculated cost for CSP is much less than five ms in 3 techniques. Yes, even if the co-owners increase to 5. Therefore, our scheme for information exchange between multiple owners in cloud computing is realistic and green.

V. CONCLUSION

The security and confidentiality of data are a situation for cloud computing users. Specifically, how addressing owners' privacy concerns and maintaining record confidentiality becomes an adventure. This article presents a Multinent Friendly Fact Organization Sharing and Conditional Spread Scheme in Cloud Computing. In our scheme, the data owner wants to encrypt his non-public data and provide him with easy access to data based on the IBBE method. Meanwhile, the data owner can define access to successful granular access coverage for attribution-based CPRE-based ciphertext. Thus the ciphertext can only be re-encrypted through a file spreader whose attributes are in the ciphertext. Meet the input access policy. We also offer a multi-way access control mechanism on ciphertext, allowing file co-owners to add their own access rules to ciphertext. In addition, we offer 3 coverage aggregation techniques that include full consent, owner preference, and majority consent to resolve privacy dispute

ISSN: 2366-1313

issues. In the future, we will decorate our schema by supporting keyword searches on the ciphertext.

REFERENCES

[1] C. S. Alliance, 2011, "Security Guidance for Critical Areas of Focus in Cloud Computing"

[2] D. Boneh and M. Franklin, 2001, ''Identity-based encryption from the Weil pairing,'', pp. 213–229.

[3] Y. Zhu, and H. Wang, 2010, ''Cryptographic role-based security mechanisms based on role-key hierarchy , pp. 314–319.

[4] Y. Zhu and S.-B Wang,. 2011, ''provably secure role-based encryption with revocation mechanism,'', pp. 697–710.

[5] 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.

[6] C. Delerablée, "Identity-based broadcast encryption with constant size ciphertexts and private keys," Proc. International Conf. on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2007), pp. 200-215, 2007.

[7] N. Paladi, C. Gehrmann, and A. Michalas, "Providing user security guarantees in public infrastructure clouds," IEEE Transactions on Cloud Computing, vol. 5, no. 3, pp. 405-419, 2017.

[8] Prasadu *Peddi (2020), MINING POSTS AND COMMENTS FROM ONLINE SOCIAL NETWORKS, Turkish Journal of Computer and Mathematics Education, Vol 11, No 3, pp: 1018-1030.*

[9] L. Jiang, and D. Guo, 2017, "Dynamic encrypted data sharing scheme based on conditional proxy broadcast re-encryption for cloud storage,", pp. 13336 – 13345.

[10] Prasadu Peddi (2019), Data Pull out and facts unearthing in biological Databases, International Journal of Techno-Engineering, Vol. 11, issue 1, pp: 25-32.