International Journal of Engineering Trends, Management & Medical Sciences
ISSN: XXXX-XXXX

SECURE DATA SHARING AND SEARCHING AT THE EDGE OF CLOUD ASSISTED IOT

Veldandi Srikanth
Assistant Professor, SVS Engineering College, Hyderabad

ABSTRACT

The rapid expansion of cloud services has made it possible to share enormous volumes of data via the use of cloud computing. While cryptographic techniques have been used to guarantee data secrecy in cloud computing, existing procedures are not adequate to enforce privacy concerns over cipher text that has many owners. Because of this, co-owners are unable to appropriately regulate whether or not data disseminators are able to really distribute their data. This study presents a concept for a multi-owner, conditional dissemination strategy for safe data group sharing in cloud computing. With the help of this technique, the data owner may securely communicate confidential information with a group of users via the cloud. If the characteristics meet the cipher text's access restrictions, the data disseminator can then share the information with a new group of users. Furthermore, we provide a multiparty access control technique that may be used with the publicly distributed cipher text. By using this technique, the co-owners of the data may add additional access restrictions to the cipher text that reflect their personal privacy preferences. Moreover, three policy aggregation strategies are offered to address the problem of privacy conflicts resulting from different access laws. These tactics consist of majority permit authority, owner priority, and complete permit. The outcomes of the security research and the trials show that, in terms of cloud computing, our solution is both workable and effective in order to guarantee the secure sharing of data with numerous owners.

I. INTRODUCTION

The advantages of abundant storage capacity and immediate access are the reasons for the growing popularity of cloud computing [1]. After combining computer infrastructure resources, it offers on-demand services over the Internet. Public cloud services are now offered by several well-known businesses, including Amazon, Google, and Alibaba. With the use of these services, both individual and business users may upload files (such as documents, movies, and images) to cloud service providers (CSPs) so they can share and access the data from anywhere at any time. Most cloud services employ access control lists (ACLs) to safeguard user privacy by limiting user access. Users may decide whether to make their data publicly available or to limit access to just those individuals they have authorized. However, since the CSP stores the data in plaintext, individuals are concerned about the security dangers. The data owner has no control over the data after it has been submitted to the CSP [2]. Sadly, the CSP is often a semi-trusted

server that complies with the rules and protocols in good faith, but it may also gather user data and use it for its own advantage without permission.

However, a variety of data consumers make extensive use of the data to understand user behavior [3]. These security concerns drive the development of practical data confidentiality protection solutions. To accomplish safe data sharing in cloud computing, access control measures must be implemented [4]. At the moment, these security and privacy issues have been resolved via the use of cryptographic techniques such attribute-based encryption (ABE) [5], identity-based broadcast encryption (IBBE) [6], and remote attestation [7]. One of the newest cryptographic techniques used in cloud computing to provide safe and precise data exchange is called ABE [8]. It has a feature that allows access control over encrypted data by assigning characteristics to decryption keys and cipher texts and using access rules. The decrypted text can only be accessed if the attribute set complies with the access policy. IBBE is another widely used technology in cloud computing [9], [10], where users may exchange their encrypted data with several recipients at once and the recipient's public key can be interpreted as any valid string, such an email address or unique identity. Indeed, for policies with an OR gate, IBBE may be considered a particular example of ABE. In contrast to ABE, which requires the secret key and cipher text to match a set of criteria, IBBE has smaller fixed policy sizes and minimal key maintenance costs, making it more suited for securely sending data to particular recipients in cloud computing.

Therefore, more users are encouraged to share their private data via the cloud as data owners may securely and effectively share data with a group of users by leveraging identities. In actuality, these encryption methods can stop malevolent users and semi-trusted CSPs from accessing the data, but they may not take cloud computing data distribution into account. The data disseminators (e.g., editor and collaborator) may share the documents with additional users, including those outside the company, in cloud collaboration scenarios like Box [11] and One Drive [12]. Data disseminators, however, are unable to alter the cipher text submitted by data owners after the data has been encrypted via the aforementioned methods [13]. The Proxy Re-Encryption (PRE) technique [14] is used in cloud computing to provide safe data distribution by assigning a re-encryption key linked to the new receivers to the CSP. With this re-encryption key, the data disseminator may share all of the data owner's data with others, which could not satisfy the practical need if the data owner only allows the data disseminator to share a specific document.

This problem may be solved by a more sophisticated idea known as additional PRE (CPRE) [15], [16], in which the data owner can impose re-encryption control on the original cipher texts and only the cipher texts meeting certain requirements can be re-encrypted with matching re-encryption keys. Nevertheless, conventional CPRE techniques are limited to supporting basic keyword conditions, making them ill-suited for complicated cloud computing scenarios. An access policy is deployed in the cipher text via attribute-based CPRE, which is suggested [17] to provide expressive conditions instead of keywords. The proxy can only re-encrypt the cipher text when the re-encryption key fits

the access policy since the re-encryption key is linked to a set of characteristics. The data owner may thereby alter the shared data's fine-grained dissemination conditions.

II. PROPOSED SYSTEM

• The suggested system presents a method for achieving multi-user cipher text group sharing and captures the essential elements of multiparty authorization specifications. The following are our scheme's contributions:

• Using attribute-based CPRE in cloud computing, the system provides fine-grained conditional dissemination across the encrypted text. The data owner customizes the first access policy before the cipher text is delivered. In accordance with their privacy choices, the data co-owners may add new access rules to the encryption text using our suggested multiparty access control technique. Therefore, the data disseminator may only re-encrypt the cipher text if the characteristics meet a sufficient number of access restrictions.

• To address privacy concerns, the system offers three strategies: majority permit, owner priority, and complete permit. In particular, the data disseminator must adhere to all access rules set out by the data owner and co-owners in the overall permission strategy. The cipher text may be shared under the majority permit approach only if the total of the access policies met by the characteristics of the data disseminator is more than or equal to the threshold value that the data owner has initially determined for the data co-owners.

• The system demonstrates the accuracy of our plan, and we run tests to gauge the success of our plan by assessing performance at each stage.

Advantages

• Since data co-owners may update the cipher texts by adding their access regulations as dissemination conditions, the data security is increased.

• Continuous policy enforcement, which enforces the data owner's access policy in both the original and updated cipher text, makes the system more secure.

2.1 ARCHITECTURE OF THE PROPOSED SYSTEM:

International Journal of Engineering Trends, Management & Medical Sciences
ISSN: XXXX-XXXX

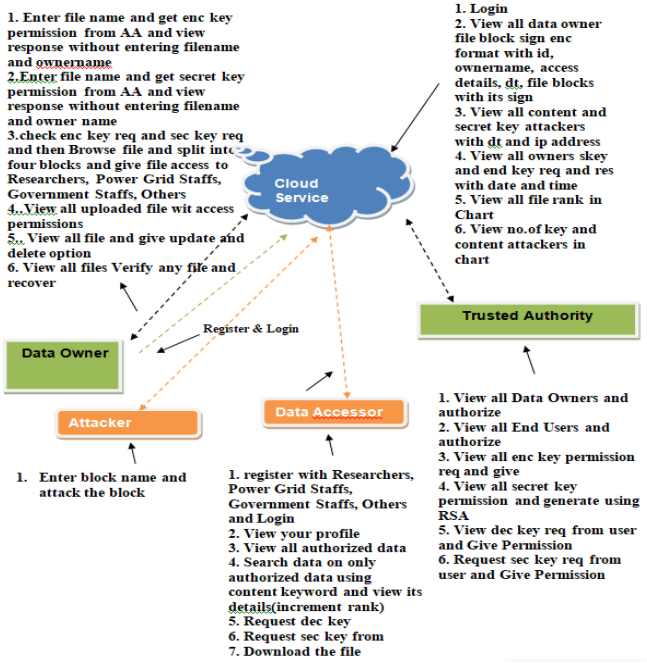

Figure 1: Architecture diagram

2.2 MODULES:

Data Owners (DO)

DO choose the access policy and use CP-ABE encryption for the data. We'll upload the encrypted data to the cloud servers. In the system, DO are presumed to be truthful.

Data Requester/Receivers (DR)

DR uses the internet to get the ciphertexts and sends the decryption request to Cloud. They can only access the plaintexts when their properties meet the ciphertext's access restrictions. Collaborating allows data requesters and recipients to obtain data that would not otherwise be available to them separately.

Cloud Servers (CS)

CS is in charge of storing enormous amounts of data. DO is not going to trust them. Therefore, in order to guarantee the confidentiality of the data, DO must set the access policy. The presumption is that CS won't work with DR.

Trusted Authority (TA)

It is AA's responsibility to register users, assess their qualities, and provide their secret key (SK) in accordance. After executing the Setup procedure, it provides each DO with the master key MK and the public key PK. It is regarded as completely reliable.

CONCLUSION

When using cloud computing, customers are concerned about data security and privacy. It becomes difficult to uphold the privacy concerns of various owners and maintain the secrecy of the data in particular. We introduce a multi-owner conditional

dissemination system and safe data group sharing in cloud computing in this research. In our approach, the data owner might conveniently use the IBBE method to encrypt their private data and distribute it with several data accessors at once. The cipher text can only be re-encrypted by data disseminators whose characteristics meet the access policy in the cipher text. In the meanwhile, the data owner may set a fine-grained access policy to the cipher text based on attribute-based CPRE. We also provide a technique for multiparty access control over the cipher text that enables the co-owners of the data to add their access rules to the cipher text. In addition, we provide three policy aggregation mechanisms to address privacy conflicts: majority permit, owner priority, and complete permit.

REFERENCES

[1] Z. Yan, X. Li, M. Wang, and A. V. Vasilakos, "Flexible data access control based on trust and reputation in cloud computing," *IEEE Transactions on Cloud Computing*, vol. 5, no. 3, pp. 485-498, 2017.

[2] B. Lang, J. Wang, and Y. Liu, "Achieving flexible and self-contained data protection in cloud computing," *IEEE Access*, vol. 5, pp. 1510- 1523, 2017.

[3] Q. Zhang, L. T. Yang, and Z. Chen, "Privacy preserving deep computation model on cloud for big data feature learning," *IEEE Transactions on Computers*, vol. 65, no. 5, pp. 1351-1362, 2016.

[4] 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.

[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] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute based encryption," *Proc. IEEE Symposium on Security and Privacy (SP'07)*, pp. 321-334, 2007.

[9] L. Liu, Y. Zhang, and X. Li, "KeyD: secure key-deduplication with identity-based broadcast encryption," *IEEE Transactions on Cloud Computing*, 2018, https://ieeexplore.ieee.org/document/8458136.

[10] Q. Huang, Y. Yang, and J. Fu, "Secure data group sharing and dissemination with attribute and time conditions in Public Clouds," *IEEE Transactions on Services Computing*, 2018, https://ieeexplore.ieee.org/document/8395392.

[11] Box, "Understanding collaborator permission levels", https://community. box.com/t5/Collaborate-By-Inviting-Others/Understanding-Collaborator-Permission-Levels/ta-p/144.

[12] Microsoft One Drive, "Document collaboration and co-authoring", https://support.office.com/en-us/article/document-collaborationand-co-authoring-ee1509b4-1f6e-401e-b04a-782d26f564a4.

[13] H. He, R. Li, X. Dong, and Z. Zhang, "Secure, efficient and finegrained data access control mechanism for P2P storage cloud," *IEEE Transactions on Cloud Computing*, vol. 2, no. 4, pp. 471-484, 2014.

[14] Z. Qin, H. Xiong, S. Wu, and J. Batamuliza, "A survey of proxy reencryption for secure data sharing in cloud computing," *IEEE Transactions on Services Computing*, 2018, https://ieeexplore.ieee.org/document/7448446.

[15] J. Son, D. Kim, R. Hussain, and H. Oh, "Conditional proxy reencryption for secure big data group sharing in cloud environment," *Proc.* of *2014 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pp. 541–546, 2014.

[16] L. Jiang, and D. Guo "Dynamic encrypted data sharing scheme based on conditional proxy broadcast re-encryption for cloud storage," *IEEE Access*, vol. 5, pp. 13336 – 13345, 2017.