AN EFFICIENT METHOD FOR DATA SHARING IN CLOUD STORAGE BY USING KEY AGGREGATE SEARCHABLE ENCRYPTION(KASE)

Akhila. H. Kumar[1] and Manjunath C R[2]

[1]PG student[1], Department of Computer Science and Engineering, Jain (Deemed –To –Be University), Bangalore, Karnataka
[2]Associate professor, Department of Computer Science and Engineering, Jain (Deemed –To –Be University), Bangalore, Karnataka

---***---

Abstract: The share of cloud data protection is the process of obtaining personal or corporate data, wherever the data is, whether it is resting or moving. But now and then, we saw data leaks or data breaches from good cloud storage with security and privacy. The encryption process that secures cloud data storage is required to share our information such as files, audio, videos, or documents to a specific user or group of users. This challenge needs to be addressed by creating robust security and privacy for cloud data storage and data sharing through an encryption process. Adaptation to cloud-sharing documents for the user or group of users requires an encryption key process to be used for the various documents. Not only the encryption keys but also the search keys must be used and users must keep their keys secure and distributed. The case highlights the concept and concept of representation, where the data owner can only share one key with the user, whether it is any type of document, large or small number of documents, and the role of the user is to move a trap in the cloud of performance testing and security analysis of shared documents, which is a secure and effective proposed provides schemes. And users are also very concerned about data sharing storage, unexplained data leaks in the cloud, and malicious attackers. Such data leaks, caused by malicious enemies or malicious cloud operators, can lead to serious breaches of personal privacy or trade secrets in the public cloud.

Keywords: cloud data security, cloud data protection share, data leakage, encryption keys, single trapdoor, KASE scheme.

1. INTRODUCTION

Companies collect large amounts of data, from confidential business, financial, and customer information to non-essential information. The ability to selectively share encrypted data with a variety of users through public cloud storage can significantly reduce security concerns with unparalleled data leaks in the cloud [1]. People face a host of security challenges, including the potential for security breaches, loss or theft of sensitive data and app crashes, and virus transmission. Nowadays, several users often share their information such as videos, audio, documents, files, folders, etc. using cloud storage [2]. The main purpose of the program is to enable efficient and secure data sharing using the concept of using cloud computing as a major problem-solving challenge. As when users try to upload files, folders, photos, videos, etc. Uploading files will produce one key and while downloading will generate another security key called cryptography cloud storage.

Here the cloud service provider is Dropbox but here the latest use is very difficult for users to use so here by taking Driver HQ as a cloud service provider which will be useful for educational and business purposes [3]. However, data encryption makes it difficult for users to search and opt for data only. Keywords provided. A common solution is to hire a searchable encryption (SE) scheme [4] where the data owner is required to encrypt potential keywords and upload them to the cloud with encrypted data, that, in retrieving data such as keyword, the user will send the corresponding keyword to the cloud.

2. EXISTING SYSTEM

By talking to users about potential data leaks in the cloud storage, it is common practice for the data owner to encrypt all data before uploading it to the cloud [5] so that the encrypted data can then be retrieved and embedded with the existing encryption keys. With the easy sharing of data with cloud storage, users are also more concerned about sudden data leaks in the cloud. PRE schemes do not support a better TRPCRE system for timely deployment with selected text transfers, flexible encryption [6], and simple computer environment encryption. The file owner can authorize the cloud server to convert the selected encrypted text on the recipient's public key into another ciphertext under the specified circumstances. Using the public-key encryption [7] real-world data set with Key Guesting Attacks Scheme and Dual-Server Keyword Search (DPAEKS), it is ready to be deployed to the operating system, providing our system with the best performance and robust security. 1 Security Analysis has shown high security, local data privacy, index and trapdoor privacy protection, and trapdoor non-connection as an appropriate process with a geometric range (EGRQ) using the concept of a functional and well-designed questionnaire. Polynomial, R-Tree, and Order-Maintenance Order [8,9]. Disadvantages of an existing system were found:

Users need to create a large number of doors and send them to the cloud to perform keyword searches on multiple files.

Communication The specified requirement for secure communication, storage, and computer complexity make such a system inefficient and ineffective.

By proposing key search key encryption and integrating the concept using the KASE concrete scheme [10] and the KAE system [11]. First, the data owner must distribute only one integration key to the user to share any number of files. Second, the user only needs to move a single integrated sequence in the cloud to create a keyword larger than any shared file number. Advantages of a valid KASE system, an advisory system that is practical and security requirements to build efficiency and security.

3. METHODOLOGY

The need to first share encrypted data in different ways often requires different encryption keys that are used for different files or documents. However, the amount of keys that must be distributed to multiple users to search for encrypted files and delete encrypted files is equal to the number of those files. Such a large amount of keys are not only distributed to users through secure channels but are also securely stored and maintained by users on their devices. Additionally, users must create a large number of loops and send them to the cloud to perform keyword searches on multiple files. Using key aggregate encryption (KASE) methods, the AES algorithm is used to upload a file to the cloud. The AES algorithm generates a public key and a private key using the key private key to upload a file. With the help of the public key and the hash key, the merge key is created; Trapdoor Keyword: The DES algorithm is used to encrypt the US key for security purposes and is based on the ranking algorithm, standard keywords are stored and Real Cloud Storage: Second, only an integrated Trapdoor must be moved in the cloud by user searches. The keyword above cloud data sharing and cloud data protection as shown in the figure above is the amount of the shared file, the method of formulating how it works, and its process as shown in Fig. 3.1 below.

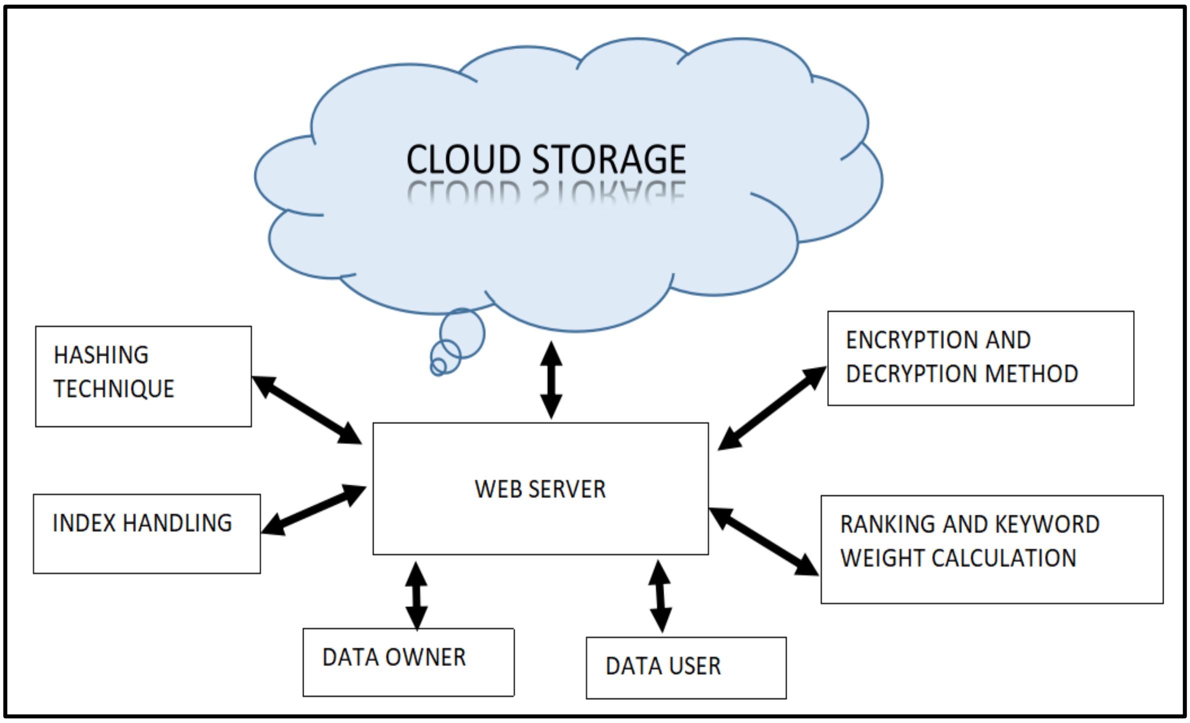

Fig 3.1 ARCHITECTURE

Fig3.1 tells us about how the data is stored in the cloud and the process of data sharing protection through encryption and decryption and search keywords by calculating keywords to make user access to his or her documents by data owner through hashing and index management.

4. CONCLUSION

Thus, future work on data security and storage is very important, as it moves our devices, data centers, business processes, and more into the cloud. It is very useful and secure for users without any conflicts. And the great advantage of using this solution is that, regardless of the size of the document, it is completely encrypted and the message is received in the user email after the user behavior profile is created. Ensuring high-quality cloud data protection through integrated security policies, organizational security culture, and cloud security solutions.

REFERENCES

[1] S. Ma, Q. Huang, M. Zhang, and B. Yang, "Efficient public-key encryption with equality test supporting flexible authorization", *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 3, pp. 458-470, Mar. 2015.

[2] Y. Li, Y. Yu, G. Min, W. Susilo, J. Ni, and K.-R. Choo, "Fuzzy identity-based data integrity auditing for reliable cloud storage systems", *IEEE Trans. Dependable Secure Comput.*, vol. 16, no. 1, pp. 72-83, Jan./Feb. 2019.

[3] [H. Li, D. Liu, Y. Dai, T. H. Luan, and X. S. Shen, "Enabling efficient multi-keyword ranked search over encrypted mobile cloud data through blind storage", *IEEE Trans. Emerg. Topics Comput.*, vol. 3, no. 1, pp. 127-138, Mar. 2015.

[4] H. Zhu, L. Wang, H. Ahmad, and X. Niu, "Key-policy attribute-based encryption with equality test in cloud computing", *IEEE Access*, vol. 5, pp. 20428-20439, 2017.

[5] Q. Wang, L. Peng, H. Xiong, J. Sun and Z. Qin, "Ciphertext-policy attribute-based encryption with delegated equality test in cloud computing", *IEEE Access*, vol. 6, pp. 760-771, 2018.

[6] Q. Wang, L. Peng, H. Xiong, J. Sun and Z. Qin, "Ciphertext-policy attribute-based encryption with delegated equality test in cloud computing", *IEEE Access*, vol. 6, pp. 760-771, 2018.

[7] Y.-M. Tseng, T.-T. Tsai, S.-S. Huang and C.-P. Huang, "Identity-based encryption with cloud revocation authority and its applications", *IEEE Trans. Cloud Comput.,2016.*

[8] Y. Sun, F. Zhang, L. Shen, and R. H. Deng, "Efficient revocable encryption against decryption key exposure", *IEEE Inf. Secure.*, vol. 9, no. 3, pp. 158-166, 2017.

[9] S. Park, K. Lee and D. H. Lee, "New constructions of revocable identity-based encryption from multilinear maps", *IEEE Trans. Inform. Forensics Security*, vol. 10, no. 8, pp. 1564-1577, Aug. 2015.

[10] Li, J. Li, X. Chen, C. Jia, and W. Lou, "Identity-based encryption with outsourced revocation in cloud computing", *IEEE Trans. Comput.*, vol. 64, no. 2, pp. 425-437, Feb. 2019.

[11] Li, Y. Shi, and Y. Zhang, "Searchable ciphertext-policy attribute-based encryption with revocation in cloud storage", *IEEE Int. J. Commun. Syst.*, 2018.