IJARSCT

ISSN (Online) 2581-9429

IJARSCT

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Impact Factor: 7.301

Volume 3, Issue 4, May 2023

Threshold Multi Keyword Search for Group Data Sharing in Cloud

Aswin K[1], Divya Shree P. K[2], Dowmika C[3], Gayathiri K. S[4], Megala V[5]

Department of Computer Science and Engineering

Dhanalakshmi Srinivansan Engineering College (Autonomous), Perambalur, India

Abstract*:* *Cloud computing provides high performance, accessibility and low cost for data storing and sharing, provides a better consumption of resources. In cloud computing, cloud service providers compromise an abstraction of infinite storage space for clients to mass data. It can help clients diminish their financial overhead of data managements by drifting the local managements system into cloud servers. However, security concerns develop the main constraint as we now outsource the storage of data, which is possibly sensitive, to cloud providers. To preserve data privacy, a mutual approach is to encrypt data files before the clients upload the encrypted data into the cloud. Cloud storage services can help clients reduce their monetary and maintenance overhead of data managements. It is complex to design a secure data sharing scheme, especially for dynamic groups in the cloud. To overcome the problem, here propose a secure data sharing scheme for frequently changed groups. In this work, an AES based encryption scheme is proposed which incorporates the cryptographic approaches with Group Data Sharing and also an anonymous control scheme to address the privacy in data as well as the user identity privacy in current access control schemes. If the group member can be revoked means, automatically change public keys of existing group and no need encrypt again the original data. Any user in the group can access data source in the cloud and revoked users does not allowed accessing the cloud again after they are revoked. Finally implement this secure distribution scheme into group data sharing environments. To reduce the computation burden on the user side, a Third Party Auditor (TPA) is introduced to verify the integrity of the cloud data on behalf of user. When owner send request for file auditing, TPA will check the file integrity using TPA verification key and send results to the owner.*

Keywords: *Data Sharing in Cloud, Group Key Verification, Group Data Sharing, Role Based Access Control, AES Encryption, User Revocation.*

REFERENCES

[1] Zhang, Cheng, Yang Xu, Yupeng Hu, Jiajing Wu, Ju Ren, and Yaoxue Zhang. "A blockchain-based multi-cloud storage data auditing scheme to locate faults." IEEE Transactions on Cloud Computing 10, no. 4 (2021): 2252-2263.

[2] Rajput, Ahmed Raza, Qianmu Li, and MiladTalebyAhvanooey. "A blockchain-based secret-data sharing framework for personal health records in emergency condition." In Healthcare, vol. 9, no. 2, p. 206.MDPI, 2021.

[3] Li, Jiaxing, Jigang Wu, Guiyuan Jiang, and ThambipillaiSrikanthan. "Blockchain-based public auditing for big data in cloud storage." Information Processing & Management 57, no. 6 (2020): 102382.

[4] Shen, Jian, Huijie Yang, PandiVijayakumar, and Neeraj Kumar. "A privacy-preserving and untraceable group data sharing scheme in cloud computing." IEEE Transactions on Dependable and Secure Computing 19, no. 4 (2021): 2198-2210.

[5] Li, Yannan, Yong Yu, Bo Yang, Geyong Min, and Huai Wu. "Privacy preserving cloud data auditing with efficient key update." Future Generation Computer Systems 78 (2018): 789-798.

[6] Shen, Jian, Jun Shen, Xiaofeng Chen, Xinyi Huang, and Willy Susilo. "An efficient public auditing protocol with novel dynamic structure for cloud data." IEEE Transactions on Information Forensics and Security 12, no. 10 (2017): 2402-2415.

[7] Yu, Yong, Man Ho Au, Giuseppe Ateniese, Xinyi Huang, Willy Susilo, Yuanshun Dai, and Geyong Min. "Identity-based remote data integrity checking with perfect data privacy preserving for cloud storage." IEEE Transactions on Information Forensics and Security 12, no. 4 (2016): 767-778.

DOI: 10.48175/IJARSCT-9852

[8] Shen, Wenting, Jia Yu, Hui Xia, Hanlin Zhang, Xiuqing Lu, and RongHao. "Light-weight and privacy-preserving secure cloud auditing scheme for group users via the third party medium." Journal of Network and Computer Applications 82 (2017): 56-64.

[9] Shen, Wenting, Guangyang Yang, Jia Yu, Hanlin Zhang, Fanyu Kong, and RongHao. "Remote data possession checking with privacy-preserving authenticators for cloud storage." Future Generation Computer Systems 76 (2017): 136-145.

[10] Tian, Hui, Fulin Nan, Hong Jiang, Chin-Chen Chang, Jianting Ning, and Yongfeng Huang. "Public auditing for shared cloud data with efficient and secure group management." Information Sciences 472 (2019): 107-125.

DOI: 10.48175/IJARSCT-9852