IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, April 2022
Impact Factor: 6.252

Privacy-Preserving Media Sharing with Scalable Access Control and Secure Deduplication in Cloud Computing

Prof. Sonali Sethi[1], Atharv Birari[2], Saurabh Bhave[3], Pravin Jadhav[4], Rohit Godse[5]
Faculty, Department of Computer Engineering [1]
Students, Department of Computer Engineering[2,3,4,5]
NBN Sinhgad School of Engineering, Pune, Maharashtra, India

Abstract: *To save cloud storage space, safe deduplication algorithms have been developed. To begin, we'll go through the AES encryption algorithm, which encrypts messages using a message-derived key. As a result, identical plaintexts generate similar ciphertexts. AES, which encompasses convergent encryption and provides precise security definitions, was proposed. Cloud computing is the advancement of sharing large amounts of data through a network. There are numerous approaches for providing data security in the cloud. Current approaches, on the other hand, are more closely tied to the ciphertext. So, in this paper, we suggest a cloud- based information collection, sharing, and restricted dissemination plan that preserves multi-owner privacy. Here, the data owner can securely share confidential information with a group of clients via the cloud.*

Keywords: Safe Deduplication Algorithms

REFERENCES

[1]. Q. Li, J. Ma, R. Li, X. Liu, J. Xiong, and D. Chen, "Secure, efficient and revocable multi-authority access control system in cloud storage," Computers Security, vol. 59, pp. 45–59, 2016.
[2]. J. Li, H. Yan, and Y. Zhang, "Certificateless public integrity checking of group shared data on cloud storage," IEEE Transactions on Services Computing, pp. 1–12, 2018.
[3]. J. Li, W. Yao, Y. Zhang, H. Qian, and J. Han, "Flexible and fine-grained attribute-based data storage in cloud computing," IEEE Transactions on Ser vices Computing, vol. 10, no. 5, pp. 785–796, Sept 2017.
[4]. J. Li, W. Yao, J. Han, Y. Zhang, and J. Shen, "User collusion avoidance cp-abe with efficient attribute revocation for cloud storage," IEEE Systems Journal, pp. 1–11, 2017.
[5]. H. Wang, Z. Zheng, L. Wu, and P. Li, "New directly revocable attribute-based encryption scheme and its application in cloud storage environment," Cluster Computing, vol. 20, no. 3, pp. 2385–2392, Sep 2017. [Online].
[6]. T. Taleb, A. Ksentini, M. Chen, and R. Jantti, "Coping With Emerging Mo bile Social Media Applications Through Dynamic Service Function Chain ing," IEEE Transactions on Wireless Communications, vol. 15, no. 4, pp. 2859–2871, Apr. 2016.
[7]. K. Yang, Z. Liu, X. Jia, and X. S. Shen, "Time-Domain AttributeBased Access Control for Cloud-Based Video Content Sharing: A Cryptographic Approach," College Short Form Name, Department of Computer Engineering 2021 44 IEEE Transactions on Multimedia, vol. 18, no. 5, pp. 940–950, May 2016
[8]. M. J. Atallah, K. B. Frikken, and M. Blanton, "Dynamic and Efficient Key Management for Access Hierarchies," in Proceedings of the 12th ACM Con ference on Computer and Communications Security, 2005, pp. 190–202.
[9]. C. Ma, Z. Yan, and C. W. Chen, "Scalable Access Control For Privacy-Aware Media Sharing," IEEE Transactions on Multimedia, vol. 21, no. 1, pp. 173–183, Jan. 2019.
[10]. H. Cui, R. H. Deng, Y. Li, and G. Wu, "Attribute-Based Storage Supporting Secure Deduplication of Encrypted Data in Cloud,"IEEE Transactions on Big Data, pp. 1–1, 2019.