IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 5, June 2022
Impact Factor: 6.252

Multi - Authority Based Approach for Manipulation of Encrypted Data in Cloud

R Mariammal[1], Venkatasubramanian C[2], Vishal Surya P A[3], Goutham Kumar M[4]
Assistant Professor, Department of Computer Science and Engineering[1]
UG Scholar, Department of Computer Science and Engineering[2,3,4]
Dhanalakshmi College of Engineering, Chennai, Tamil Nadu, India

Abstract: *In this paper, we address the protection concerns of cloud storage under the scenario where users encrypt-then-outsource data, share their outsourced data with other users, and so the service provider may be queried for searching and retrieval of encrypted data. Because the main distinctive, we propose a security approach for storage, sharing, and retrieval of encrypted data within the fully as constructed supported attribute-based encryption (ABE) thus enabling access control mechanisms over both the encrypted data and also for the data retrieval task through search access control. Efforts have studied problems around this application scenario on different fronts: efficiency, flexibility, reliability, and security. Our suggested secure Multi-authority CP-ABKS (MABKS) system addresses such limitations and minimizes the computation and storage burden on resource-limited devices in cloud systems. Additionally, the MABKS system is extended to support malicious attribute authority tracing and attribute update. proposed a practical CP-ABE scheme, which offers user revocation and attributes updates. We proposed an efficient and feasible MABKS system to support multiple authorities, to avoid having performance bottlenecks at one point in cloud systems. Furthermore the presented MABKS system allows us to trace malicious.*

Keywords: Cloud Storage.

REFERENCES

[1]. A. Bagherzandi, B. Hore, and S. Mehrotra, Search over Encrypted Data. Boston, MA, USA: Springer, 2011, pp. 1088–1093.
[2]. H. Pham, J. Woodworth, and M. A. Salehi, ‘‘Survey on secure search over encrypted data on the cloud,’’ Concurrency Comput. Pract. Exper., vol. 31, p. 1– 15, Apr. 2019.
[3]. R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, ‘‘Searchable symmetric encryption: Improved definitions and efficient constructions,’’ in Proc. 13th ACM Conf. Comput. Commun. Secur., New York, NY, USA, 2011, pp. 79–88, 2006.
[4]. M. Zeng, H.-F. Qian, J. Chen, and K. Zhang, ‘‘Forward secure public key encryption with keyword search for outsourced cloud storage,’’ IEEE Trans. Cloud Comput., early access, Sep. 27, 2019, doi: 10.1109/TCC.2019.2944367.
[5]. S. Kamara, C. Papamanthou, and T. Roeder, ‘‘Cs2: A searchable cryptographic cloud storage system,’’ Microsoft Res., Redmond, WA, USA, Tech. Rep. MSR-TR-2011-58, May 2011.
[6]. W. Song, B. Wang, Q. Wang, Z. Peng, W. Lou, and Y. Cui, ‘‘A privacypreserved full-text retrieval algorithm over encrypted data for cloud storage applications,’’ J. Parallel Distrib. Comput., vol. 99, pp. 14–27, Jan. 2017.
[7]. A. G. Kumbhare, Y. Simmhan, and V. Prasanna, ‘‘Designing a secure storage repository for sharing scientific datasets using public clouds,’’ in Proc. 2nd Int. workshop Data Intensive Comput. Clouds, 2011, pp. 31–40.
[8]. Z. Yang, J. Tang, and H. Liu, ‘‘Cloud information retrieval: Model description and scheme design,’’ IEEE Access, vol. 6, pp. 15420–15430, 2018.
[9]. H. Yin, J. Zhang, Y. Xiong, L. Ou, F. Li, S. Liao, and K. Li, ‘‘CP-ABSE: A ciphertext-policy attribute-based searchable encryption scheme,’’ IEEE Access, vol. 7, pp. 5682–5694, 2019.
[10]. A. Sahai and B. Waters, ‘‘Fuzzy identity-based encryption,’’ in Advances in Cryptology (Lecture Notes in Computer Science), vol. 3494, R. Cramer, Ed. Berlin, Germany: Springer-Verlag, 2005, pp. 457–473.