IJARSCT

ISSN (Online) 2581-9429

IJARSCT

Impact Factor: 7.301

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

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

Volume 3, Issue 2, September 2023

Integrated Approach for Providing Data Security Verification Over Encrypted Cloud Data

Mr. Kuna Suresh

Department of Computer Science and Systems Engineering (A), Andhra University, Visakhapatnam, India

Abstract*:* *The cloud has recently attracted a lot of user attention from both small and large businesses, including those in software, BPO, healthcare, schools, colleges, and many other industries. For data storage and access from remote places linked to one another from a central server with the aid of the internet, all of these organisations attempt to adopt this centralised cloud server. Because all data is stored remotely and only occasionally accessed locally, the confidentiality of data is crucial to cloud service providers. As is common knowledge, no cloud service provider currently offers data privacy through encryption and message digests to enable data authorisation. almost all businesses An untrusted user can query data files of interest by sending encrypted keywords as a search query to the cloud server. Try to search the data in a secure manner over encrypted cloud data. In this dishonest cloud environment, the returned query results may occasionally be correct, incorrect, or partial. As everyone is aware, cloud servers today nearly actively withhold some qualified results in order to conserve computational resources and communication overhead. In this research, we presented and analysed a safe, practical, and fine-grained query results verification mechanism, by which the query user, given an encrypted query results set, not only can confirm the integrity of each data file, but also determines the overall number of qualifying data files, which are not returned if the set is not finished before the decryption procedure. This served as our primary inspiration for creating a brand-new secure verification object for encrypted cloud storage. Here, the short signature key is created using the message digest method MD5, which is also used to confirm the data's authenticity. We tested our proposed model in a variety of ways, and the results demonstrate that it is a useful and effective system.*

Keywords: cloud

REFERENCES

[1] P. Mell and T. Grance, “The nist definition of cloud computing,” http://dx.doi.org/10.602/NIST.SP.800-145.

[2] K. Ren, C. Wang, and Q. Wang, “Security challenges for the public cloud,” IEEE Internet Computing, vol. 16, no. 1, pp. 69–73, 2012.

[3] S. Kamara and K. Lauter, “Cryptographic cloud storage,” in Springer RLCPS, January 2010.

[4] D. Song, D. Wagner, and A. Perrig, “Practical techniques for searches on encrypted data,” in IEEE Symposiumon Security and Privacy, vol. 8, 2000, pp. 44–55.

[5] E.-J.Goh, “Secure indexes,” IACR ePrint Cryptography Archive, http://eprint.iacr.org/2003/216, Tech. Rep., 2003.

[6] D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano, “Public-key encryption with keyword search,” in EUROCRYPR, 2004, pp. 506–522.

[7] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, “Searchable symmetric encryption: improved deinitions and efficient constructions,” in ACM CCS, vol. 19, 2006, pp. 79–88.

[8] M. Bellare, A. Boldyreva, and A. O’Neill, “Deterministic and efficiently searchable encryption,” in Springer CRYPTO, 2007.

[9] K. Kurosawa and Y. Ohtaki, “Uc-secure searchable symmetric encryption,” Lecture Notes in Computer Science, vol. 7397, pp. 258–274, 2012.

DOI: 10.48175/IJARSCT-13028

[10] P. Xu, H. Jin, Q. Wu, and W. Wang, “Public-key encryption with fuzzy keyword search: A provably secure scheme under keyword guessing attack,” IEEE Transactions on Computers, vol. 62, no. 11, pp. 2266–2277, 2013.

[11] S. Kamara and C. Papamanthou, “Parallel and dynamic searchable symmetric encryption,” in Financial Cryptography and Data Security. Springer Berlin Heidelberg, 2013, pp. 258–274.

[12] M. Naveed, M. Prabhakaran, and C. A. Gunter, “Dynamic searchable encryption via blind storage,” in IEEE S&P, May 2014, pp. 639–654.

[13] C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, “Secure ranked keyword search over encrypted cloud data,” in IEEE ICDCS, 2010, pp. 253–262.

[14] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, “Privacy-preserving multi-keyword ranked search over encrypted cloud data,” in IEEE INFOCOM, 2011, pp. 829–837.

[15] W. Sun, B. Wang, N. Cao, M. Li, W. Lou, Y. T. Hou, and H. Li, “Privacy-preserving multi-keyword text search in the cloud supporting similarity-based ranking,” in ACM ASIACCS, 2013.

[16] B. Wang, S. Yu, W. Lou, and Y. T. Hou, “Privacy-preserving multi-keyword fuzzy search over encrypted data in the cloud,” in IEEE INFOCOM, 2014, pp. 2112–2120.

DOI: 10.48175/IJARSCT-13028