IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, June 2022
Impact Factor: 6.252

Integrity Auditing for Multi-Copy in Cloud Storage Based on Red-Black Tree

Mr. R.Arunachalam[1], Deepika Thennarasu[2], Dhanasri Natarajan[3], Madhumitha Baskar[4]
Assistant Professor, Department of Computer Science and Engineering[1]
Students, Department of Computer Science and Engineering[2,3,4]
Anjalai Ammal Mahalingam Engineering College, Kovilvenni, Tiruvarur, Tamil Nadu, India

Abstract: *With the rapid development of cloud storage, cloud users are willing to store data in the cloud storage system, and at the same time, the requirements for the security, integrity, and availability of data storage are getting higher and higher. Although many cloud audit schemes have been proposed, the data storage overhead is too large and the data cannot be dynamically updated efficiently when most of the schemes are in use. In order to solve these problems, a cloud audit scheme for multi-copy dynamic data integrity based on red-black tree full nodes is proposed. This scheme uses ID-based key authentication, and improves the classic Merkel hash tree MHT to achieve multi-copy storage and dynamic data manipulation, which improves the efficiency of real-time dynamic data update (insertion, deletion, modification). The third-party audit organization replaces users to verify the integrity of data stored on remote cloud servers, which reduces the computing overhead and system communication overhead. The security analysis proves that the security model based on the CDH problem and the DL problem is safe. Judging from the results of the simulation experiment, the scheme is safe and efficient.*

Keywords: Cloud storage, data integrity auditing, red-black tree, dynamic data update.

REFERENCES

[1]. W. Shen, J. Yu, H. Xia, H. Zhang, X. Lu, and R. Hao, ''Light-weight and privacy-preserving secure cloud auditing scheme for group users via the third party medium,'' J. Netw. Comput. Appl., vol. 82, pp. 56–64, Mar. 2017.

[2]. M. Alshehri, A. Bhardwaj, M. Kumar, S. Mishra, and J. Gyani, ''Cloud and IoT based smart architecture for desalination water treatment,'' Environ. Res., vol. 195, Apr. 2021, Art. no. 110812, doi: 10.1016/ j.envres.2021.110812.

[3]. S. Srivastava, S. Saxena, R. Buyya, M. Kumar, A. Shankar, and B. Bhushan, ''CGP: Cluster-based gossip protocol for dynamic resource environment in cloud,'' Simul. Model. Pract. Theory, vol. 108, Apr. 2021, Art. no. 102275, doi: 10.1016/j.simpat.2021.102275.

[4]. K. He, J. Chen, Q. Yuan, S. Ji, D. He, and R. Du, ''Dynamic group-oriented provable data possession in the cloud,'' IEEE Trans. Dependable Secure Comput., early access, Jul. 2, 2019, doi: 10.1109/TDSC.2019.2925800.

[5]. M. Kumar, M. Alshehri, R. AlGhamdi, P. Sharma, and V. Deep, ''A DE-ANN inspired skin cancer detection approach using fuzzy C-means clustering,'' Mobile Netw. Appl., vol. 25, no. 4, pp. 1319–1329, Aug. 2020, doi: 10.1007/s11036-020-01550-2.

[6]. L. Zhou, A. Fu, G. Yang, H. Wang, and Y. Zhang, ''Efficient certificateless multi-copy integrity auditing scheme supporting data dynamics,'' IEEE Trans. Dependable Secure Comput., early access, Aug. 4, 2020, doi: 10. 1109/TDSC.2020.3013927.

[7]. C. Dhasarathan, M. Kumar, A. K. Srivastava, F. Al-Turjman, A. Shankar, and M. Kumar, ''A bio-inspired privacy-preserving framework for healthcare systems,'' J. Supercomput., early access, Mar. 19, 2021, doi: 10.1007/ s11227-021-03720-9.

[8]. L. Krithikashree and S. Manisha, ''Audit cloud: Ensuring data integrity for mobile devices in cloud storage,'' IEEE Trans. Depend. Sec. Comput., pp. 1–5, Sep. 2018, doi: 10.1109/ICCCNT.2018.8493963.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, June 2022
Impact Factor: 6.252

[9]. L. Deng, B. Yang, and X. Wang, ''A lightweight identity-based remote data auditing scheme for cloud storage,'' IEEE Access, vol. 8, pp. 206396–206405, 2020, doi: 10.1109/ACCESS.2020.3037696.

[10]. S. Peng, F. Zhou, Q. Wang, Z. Xu, and J. Xu, ''Identity-based public multireplica provable data possession,'' IEEE Access, vol. 5, pp. 26990–27001, 2017, doi: 10.1109/ACCESS.2017.2776275.

[11]. A. Bhardwaj, S. B. H. Shah, A. Shankar, M. Alazab, M. Kumar, and T. R. Gadekallu, ''Penetration testing framework for smart contract blockchain,'' Peer-Peer Netw. Appl., early access, Sep. 5, 2020, doi: 10. 1007/s12083-020-00991-6.

[12]. P. Shen, C. Li, and Z. Zhang, ''Research on integrity check method of cloud storage multi-copy data based on multi-agent,'' IEEE Transl. Content Mining, vol. 4, no. 8, pp. 17170–17178, 2020, doi: 10.1109/ACCESS. 2020.2966803.

[13]. Y. Luo, M. Xu, S. Fu, D. Wang, and J. Deng, ''Efficient integrity auditing for shared data in the cloud with secure user revocation,'' in Proc. IEEE Trustcom/BigDataSE/ISPA, Aug. 2015, pp. 434–442, doi: 10.1109/ Trustcom.2015.404.

[14]. R. Rabaninejad, S. M. Sedaghat, M. Ahmadian Attari, and M. R. Aref, ''An ID-based privacy-preserving integrity verification of shared data over untrusted cloud,'' in Proc. 25th Int. Comput. Conf., Comput. Soc. Iran (CSICC), Jan. 2020, pp. 1–6, doi: 10.1109/CSICC49403.2020.9050098. 75130 VOLUME 9, 2021 Z. Liu et al.: Integrity Auditing for Multi-Copy in Cloud Storage Based on Red-Black Tree

[15]. C.-T. Hunag, C.-Y. Yang, C.-Y. Weng, Y.-W. Chen, and S.-J. Wang, ''Secure protocol for identity-based provable data possession in cloud storage,'' in Proc. IEEE 4th Int. Conf. Comput. Commun. Syst. (ICCCS), Feb. 2019, pp. 327–331, doi: 10.1109/CCOMS.2019.8821766

[16]. C. Liu, J. Chen, L. Yang, X. Zhang, and R. Kotagiri, ''Authorized public auditing of dynamic big data storage on cloud with efficient verifiable fine-grained updates,'' IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 9, pp. 2234–2244, Sep. 2014.

[17]. H. Jin, H. Jiang, and K. Zhou, ''Dynamic and public auditing with fair arbitration for cloud data,'' IEEE Trans. Cloud Comput., vol. 6, no. 3, pp. 680–693, Jul. 2018, doi: 10.1109/TCC.2016.2525998.

[18]. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, ''Provable data possession at untrusted stores,'' in Proc. 14th ACM Conf. Comput. Commun. Secur. (CCS), 2007, pp. 598–609.

[19]. Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, ''Enabling public auditability and data dynamics for storage security in cloud computing,'' IEEE Trans. Parallel Distrib. Syst., vol. 22, no. 5, pp. 847–859, May 2011.

[20]. A. F. Barsoum and M. A. Hasan, ''Provable multicopy dynamic data possession in cloud computing systems,'' IEEE Trans. Inf. Forensics Security, vol. 10, no. 3, pp. 485–497, Mar. 2015.

[21]. M. Sookhak, F. R. Yu, and A. Y. Zomaya, ''Auditing big data storage in cloud computing using divide and conquer tables,'' IEEE Trans. Parallel Distrib. Syst., vol. 29, no. 5, pp. 999–1012, May 2018.

[22]. X. Yang, T. Liu, P. Yang, F. An, M. Yang, and L. Xiao, ''Public auditing scheme for cloud data with user revocation and data dynamics,'' in Proc. IEEE 2nd Inf. Technol., Netw., Electron. Autom. Control Conf. (ITNEC), Dec. 2017, pp. 813–817, doi: 10.1109/ITNEC.2017.8284847.

[23]. M. Long, Y. Li, and F. Peng, ''Integrity verification for multiple data copies in cloud storage based on spatiotemporal chaos,'' Int. J. Bifurcation Chaos, vol. 27, no. 4, Apr. 2017, Art. no. 1750054.

[24]. M. Long, Y. Li, and F. Peng, ''Dynamic provable data possession of multiple copies in cloud storage based on full-node of AVL tree,'' Int. J. Digit. Crime Forensics, vol. 11, no. 1, pp. 126–137, Jan. 2019.

[25]. R. Curtmola, O. Khan, R. Burns, and G. Ateniese, ''MR-PDP: Multiplereplica provable data possession,'' in Proc. 28th Int. Conf. Distrib. Comput. Syst., Jun. 2008, pp. 411–420.

[26]. A. Barsoum and M. Hasan, ''On verifying dynamic multiple data copies over cloud servers,'' Dept. Elect. Comput. Eng., Tech. Rep., 2011.

[27]. H. Shacham and B. Waters, ''Compact proofs of retrievability,'' J. Cryptol., vol. 26, no. 3, pp. 442–483, Jul. 2013.

[28]. J. Shen, J. Shen, X. Chen, X. Huang, and W. Susilo, ''An efficient public auditing protocol with novel dynamic structure for cloud data,'' IEEE Trans. Inf. Forensics Security, vol. 12, no. 10, pp. 2402–2415, Oct. 2017.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, June 2022
Impact Factor: 6.252

[29]. W. Shen, J. Qin, J. Yu, R. Hao, and J. Hu, ‘‘Enabling identity-based integrity auditing and data sharing with sensitive information hiding for secure cloud storage,’’ IEEE Trans. Inf. Forensics Security, vol. 14, no. 2, pp. 331–346, Feb. 2019, doi: 10.1109/TIFS.2018.2850312.

[30]. Y. Zhang, J. Ni, X. Tao, Y. Wang, and Y. Yu, ‘‘Provable multiple replication data possession with full dynamics for secure cloud storage,’’ Concurrency Comput., Pract. Exper., vol. 28, no. 4, pp. 1161–1173, Mar. 2016, doi: 10. 1002/cpe.3573.

[31]. J. Li, H. Yan, and Y. Zhang, ‘‘Efficient identity-based provable multi-copy data possession in multi-cloud storage,’’ IEEE Trans. Cloud Comput., early access, Jul. 16, 2019, doi: 10.1109/TCC.2019.2929045.

[32]. T. Wu, G. Yang, Y. Mu, F. Guo, and R. H. Deng, ‘‘Privacy-preserving proof of storage for the pay-as-you-go business model,’’ IEEE Trans. Dependable Secure Comput., vol. 18, no. 2, pp. 563–575, Mar. 2021, doi: 10. 1109/TDSC.2019.2931193. [33] J. Li, J. Li, D. Xie, and

[33]. Z. Cai, ‘‘Secure auditing and deduplicating data in cloud,’’ IEEE Trans. Comput., vol. 65, no. 8, pp. 2386–2396, Aug. 2016.

[34]. The Pairing-Based Cryptography(PBC) Library. Accessed: 2020. [Online]. Available: https://crpto.stanford.edu/pbc/download.html

[35]. The GNU Multiple Precision Arithmetic Library (GMP). Accessed: 2020. [Online]. Available: http://gmplib.org