

A Secure Data Deduplication in Cloud Using Hashing and AES Algorithm

**Mahajan Mayur Pradeep¹, Bhujbal Siddhesh Vasant², Abhishek Ganpat Wadhai³,
Patil Sanyukta Madan⁴, Prof. Ravindra Borhade⁵**

Students, Department of Information Technology^{1,2,3,4}

Assistant Professor, Department of Information Technology^{1,2,3,4}

Smt. Kashibai Navale College of Engineering, Pune, Maharashtra, India

Savitribai Phule Pune University, Pune, Maharashtra, India

Abstract: Data de-duplication is a way used to compress data helping withinside the elimination of reproduction copies of data. It has been powerful in cloud garage; it decreases the specified garage area to steady such facts through thinking about de-duplication this concurrent technique has been projected. In the identical way, introducing fewer new replica exams for engineers ought to growth new de-duplication improvement assisting techniques. Security research have proven that this approachment is steady regarding the descriptions proven withinside the projected protection model. This paper will actualize a prototype of a suggested, sanctioned replica test plan and carry out experiments the use of the prototype. The look at will display that the proposed prototype reasons inconsequential overhead-differentiated archetypal processes. This paper offers and analyses a brand new scheme to deal with the difficulty of eternal cloud garage get right of entry to structures through imparting AES Algorithm primarily based totally solution. Addressing the difficulty of Data garage withinside the latest instances is the intention of the paper and is being completed the use of the latest AES Algorithm. Data protection and time constraint for facts retrieval from the cloud server is likewise taken under consideration whilst enforcing the scheme.

Keywords: Deduplication, Storage, Route key, AES Algorithm.

REFERENCES

- [1]. NIST, "NIST Brief Comments on Recent Cryptanalytic Attacks on Secure Hashing Functions and Continued Security Provided by SHA-1", 25th August 2004, http://csrc.nist.gov/groups/ST/toolkit/documents/shs/hash_standards_comments.pdf
- [2]. Federal Information Processing Standards Publication 180-3, "SECURE HASH STANDARD", October 2008, http://csrc.nist.gov/publications/fips/fips180-3/fips180-3_final.pdf
- [3]. OpenSSL Source Code, <http://www.openssl.org/source>
- [4]. N. Ferguson et al, "The Skein Hash Function Family", Version 1.3, 1st October 2010, <http://www.schneier.com/skein1.3.pdf>
- [5]. N. Jeber, Jalal. (2019). The Future of Cloud Computing Google Drive. 10.13140/RG.2.2.26342.06724.
- [6]. Burramukku, Tirapathi & Ramya, U. & Sekhar, M.V.P.. (2016). A comparative study on data deduplication techniques in cloud storage. 8. 18521-18530.
- [7]. Ku, Chan-I & Luo, Guo-Heng & Chang, Che-Pin & Yuan, Shyan-Ming. (2013). File Deduplication with Cloud Storage File System. 280-287. 10.1109/CSE.2013.52.
- [8]. N. Baracaldo, E. Androulaki, J. Glider, A. Sorniotti, "Reconciling end-to-end confidentiality and data reduction in cloud storage," Proc. ACM Workshop on Cloud Computing Security, pp. 21–32, 2014.
- [9]. C. Wang, Z. Qin, J. Peng, and J. Wang, "A novel encryption scheme for data deduplication system," Proc. International Conference on Communications, Circuits and Ssystems (ICCCAS), pp. 265–269, 2010.
- [10]. J. R. Douceur, A. Adya, W. J. Bolosky, D. Simon, and M. Theimer, "Reclaiming space from duplicate files in a serverless distributed file system," Proc. International Conference on Distributed Computing Systems (ICDCS), pp. 617–624, 2002.

- [11]. D. T. Meyer, and W. J. Bolosky, "A study of practical deduplication," Proc. USENIX Conference on File and Storage Technologies, 2011.
- [12]. A. Rahumed, H. C. H. Chen, Y. Tang, P. P. C. Lee, J. C. S. Lui, "A secure cloud backup system with assured deletion and version control," Proc. International Workshop on Security in Cloud Computing, 2011.
- [13]. Sheetal U.Jonwal,Pratibha P.Shingar,:"Advanced Encryption standard(AES) implementation on FPGA with hardware in loop", International Conference on Trends in Electronics and Informatics,ICEI 2017,DOI:10.1109/ICOEI.2017.8300776.