IJARSCT

ISSN (Online) 2581-9429

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

Impact Factor: 6.252

Volume 2, Issue 1, November 2022

Enabling Identity-based Integrity Auditing and Data Sharing with Sensitive Information Hiding for Secure Cloud Storage

Prof. C. P Lachake[1], Shinde Balaji[2], Ingle Shrikant[3], Shinde Shradha[4], Vedant Barapatre[5]

Professor, Department Of Computer Engineering[1]

Students, Department Of Computer Engineering[2,3,4,5]

SKN Sinhgad Institute of Technology and Science, Kusgaon (BK), Pune, Maharashtra, India

Abstract: *A data storage server, such as a cloud server, can demonstrate to a verifier that it is honestly storing the data of a data owner by using remote data integrity checking (RDIC). Numerous RDIC protocols have been put out in the literature to this point, however the most of these designs have a sophisticated key management problem, meaning they depend on pricy public key infrastructure (PKI), which could make it difficult to implement RDIC in practise. In order to simplify the system and lower the cost of setting up and maintaining the public key authentication framework in PKI based RDIC schemes, we suggest a novel architecture of the identity-based (ID-based) RDIC protocol in this study. We formalise ID-based RDIC, along with its security model, which includes protection from rogue cloud servers and zero knowledge privacy from a third-party verification. During the RDIC procedure, the proposed ID-based RDIC protocol does not reveal any information about the stored data to the verifier. The new design achieves zero knowledge privacy against a verifier and is demonstrated to be secure against the malicious server in the general group model. Extensive security research and implementation results show that the suggested protocol is practicable in real-world applications and provably secure. We Extend This Work with Group Management, Forward and Backward Secrecy by Time Duration, and File Recovery When Data Integrity Checking Fault Occurs.*

Keywords: Cloud Storage

REFERENCES

[1]. P. Mell, T. Grance, Draft NIST working definition of cloud computing, Reference on June. 3rd, 2009. http://csrc.nist.gov/groups/SNC/cloudcomputing/index.html.

[2]. Cloud Security Alliance. Top threats to cloud computing. http://www.cloudsecurityalliance.org, 2010.

[3]. M. Blum, W. Evans, P.Gemmell, S. Kannan, M. Naor, Checking the correctness of memories. Proc. of the 32nd Anual Symposium on Foundations foVomputers, SFCS 1991, pp. 90–99, 1991.

[4]. G. Ateniese, R. C. Burns, R. Curtmola, J. Herring, L. Kissner, Z. N.J. Peterson, D. X. Song, Provable data possession at untrusted stores. ACM Conference on Computer and communications Security, 598-609,2007.

[5]. G. Ateniese, R. C. Burns, R. Curtmola, J. Herring, O. Khan, L. Kissner, Z. N. J. Peterson, and D. Song, Remote data checking using provable data possession. ACM Trans. Inf. Syst. Secur., 14, 1–34, 2011.

[6]. G. Ateniese, R. C. Burns, R. Curtmola, J. Herring, O. Khan, L. Kissner, Z. N. J. Peterson, and D. Song, Remote data checking using provable data possession. ACM Trans. Inf. Syst. Secur., 14, 1–34, 2011.

[7]. A.Juels, and B. S. K. Jr. Pors, proofs of retrievability for large files.Proc.of CCS 2007, 584-597, 2007.

[8]. H. Shechem, and B. Waters, Compact proofs of retrievability. Proc. of Cryptology-ASIACRYPT 2008, LNCS 5350, pp. 90-107, 2008.

[9]. G. Ateniese, S. Kamara, J. Katz, Proofs of storage from homomorphicidentification protocols. Proc. of ASIACRYPT 2009, 319-333, 2009.

[10]. A. F. Barsoum, M. A. Hasan, Provable multicopy dynamic data possession in cloud computing systems, IEEE Trans. on Information Forensics and Security, 10(3): 485–497, 2015

DOI: 10.48175/568