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

A Cloud Secure Storage Mechanism Based on Data Dispersion and Encryption

Dinesh Kumar P[1] and Sneha T[2]
Assistant Professor, Department of Science and Computer Engineering[1]
Student, Department of Science and Computer Engineering[2]
Anjalai Ammal Mahalingam Engineering College, Kovilvenni, Tiruvarur, Tamil Nadu, India

Abstract: *This describes cloud storage system, it support for rapid development of cloud computing data leakage prevention algorithm and it implemented secure storage mechanism. CSSM adopted a hierarchical management approach and combined user password with secret sharing to prevent cryptographic materials leakage. Advanced encryption standard algorithm(AES) is implemented for encryption of data. The proposed scheme ensuring the reduced overhead and latency in system. The objective is to secure the cloud data with reduced leakage system. The main objective of the proposed mechanism is to secure cloud storage against data breach, which may be the result of targeted attack or management negligence (e.g. misconfiguration), in case hackers even some malicious administrator is able to steal user data.*

Keywords: Cloud computing, storage security, key management, data dispersion, data encryption.

REFERENCES

[1]. A. Bhardwaj, F. Al-Turjman, M. Kumar, T. Stephan and L. Mostarda, "Capturing-the invisible(CTI): Behavior-based attacks recognition in IoT-oriented industrial control systems," IEEE Access, vol. 8, pp. 104956–104966, 2020.

[2]. M. Kumar, A. Rani, and S. Srivastava, "Image forensics based on lighting estimation," Int. J. Image Graph., volume 19, no.3, July 2019, Art. no. 1950014.

[3]. M. Kumar, S. Srivastava, and N. Uddin, "Image forensic based on lighting estimation," Austral. J. Forensic Sci., volume 51, no.3, pp. 243–250, August 2017.

[4]. J. Li, Y. Zhang, X. Chen, and Y. Xiang, "Secure attribute-based data sharing for resource-limited users in cloud computing," Computer Secure volume 72, pp. 1–12, January 2018.

[5]. Y. Zhang, X. Chen, J. Li, D. S. Wong, H. Li, "Ensuring attribute privacy protection and fast decryption for outsourced data security in mobile cloud computing," volume 379, pp. 42–61, February 2017.

[6]. The OpenStack Project. OSSA-2015-006: Unauthorized Delete of Versioned Swift Object. Accessed: April. 14, 2015. [Online]. Available:https://security.openstack.org/ossa/OSSA-2015-006.html

[7]. The OpenStack Project. OSSA-2015-016: Information Leak Via Swift Tempurls. Accessed: August 26, 2015. [Online]. Available:https://security.openstack.org/ossa/OSSA-2015-016.html

[8]. The OpenStack Project. Possible Glance Image Exposure Via Swift. Accessed: February 23, 2015. [Online]. Available: https://wiki. openstack.org/wiki/OSSN/OSSN-0025

[9]. Cloud Security Alliance. Top Threats to Cloud Computing: Deep Dive. Accessed: August 8, 2018. [Online]. Available:https://downloads.cloudsecurityalliance.org/assets/research/top-threats/top-threats-to-cloudcomputing-deep-dive.pdf

[10]. The OpenStack Project. OpenStack Security Advisories. Accessed: February 2, 2015. [Online]. Available:https://security.openstack.org/ossalist. Html