Secure Role Based Access Control Data Sharing Approach and Cloud Environment

Om Shama[1], Usama Baig[2], Raman Chandak[3]

Students, Department of Computer Engineering [1]

Professor, Department of Computer Engineering[2,3]

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

Abstract: *the primary objective of cloud storage is to maintain data integrity, which involves implementing measures to prevent unauthorized access and ensuring that data can be regenerated if mishandled. To achieve this, a proxy server will be assigned the task of protecting and restoring data in case of unauthorized modifications. Users' data will be stored in both public and private areas of the cloud, with only public data being accessible to users and private data being kept more secure. Cloud storage offers users various redundancy configurations to balance performance and fault tolerance, with data availability being critical in distributed storage systems, especially when node failures are common in real-life scenarios. In this research, a proposed aes 128 encryption algorithm and role-based access control (rbac) scheme are explored to provide secure data storage and sharing, as well as a secure user access policy. Additionally, a backup server approach is used as a proxy storage server for ad hoc data recovery for all distributed data servers. The experiment's analysis is proposed in both public and private cloud environments, utilizing keywords such as rbac, elgamal encryption scheme, proxy key generation, advanced encryption standard (aes), and more.*

Keywords: Cloud

REFERENCES

[1]. Wei Li, Kaiping Xue, Yingjie Xue, And Jianan Hong, "TACS: A Robust And Verifiable Threshold Multiauthority Access Control System In Public Cloud Storage, IEEE Transactions On Parallel And Distributed Systems, VOL.24, No. 06, October 2017.

[2]. Taeho Jung, Xiang-yang Li, Zhiguo Wan, And Meng Wan, "Control Cloud Data Access Privilege And Anonymity With Fully Anonymous Attribute-based Encryption", IEEE Transactions On Information Forensics And Security, VOL. 10, No. O1, January 2017.

[3]. S. Kamara And K. Lauter, "Cryptographic Cloud Storage," In Proceedings Of The 14th Financial Cryptography And Data Security. Springer, 2010, Pp. 136-149.

[4]. B. Wang, B. Li, And H. Li, "Panda: Public Auditing For Shared Data With Efficient User Revocation InThe Cloud, IEEE Transactions On Services Computing, Vol. 8, No. 1, Pp. 92-106, 2015.

[5]. I. Yuan And S. Yu, "Public Integrity Auditing For Dynamic Data Sharing With Multiuser Modification," IEEE Transactions On Information Forensics And Security, Vol. 10, No. 8, Pp. 1717 - 1726, Aug. 2015.

[6]. Y. Zhu, H.G. Ahn, H. Hu, S.S. Yau, H.J. An, And C.J.Hu, "Dynamic Audit Services For Outsourced Storages In Clouds," IEEE Transactions On Services Computing, Vol.6, No. 2, Pp. 409-428, 2013.

[7]. C. Wang, S. Chow, Q. Wang, K. Ren, And W. Lou, "Privacy-preserving Public Auditing For Secure Cloud Storage," IEEE Transactions On Computers, Vol. 62, No.2, Pp. 362-375, 2013.

[8]. N. AttraPadung, B. Libert, And E. Pana_eu, "Expressive Key Policy Attribute-based Encryption With Constantsize Cipher Texts." In Proceedings Of The 14th International Conference On Practice And Theory In Public Key Cryptography. Springer, 2011, Pp. 90-108.

[9]. T. Jung, X. Li, Z. Wan, And M. Wan, "Privacy Preserving Cloud Data Access WithMultiauthorities," In Roceedings Of The 32nd Ibe International ConterenceOn Computer Communications. Bbs. 2013. Do 2625-2633.

DOI: 10.48175/IJARSCT-9425