IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 6, May 2023

To Ensure Data Security and Efficient Data Access Control for Cloud Storage using Immediate Revocable Timestamp MA-ABE Scheme

Prof. Srinath G M, Anusha A, Bhargavi B G, Deeksha M V, Enturi Vyshnavi
Department of Computer Science and Engineering
S.J.C Institute of Technology, Chickballapur, India

Abstract: The achievement for the fine-grained entry control over data and for its guarantee of data security. Multi authority Attribute based encryption schemes not suitable for the devices with resource constrained, due to it is based on expensive bilinear pairing. The major limitation of Multi-authority-ABE scheme is attribute cancellation that is revocation of attributes. Using the elliptic curves cryptography and Diffie Hellman Problem to propose an "To Ensure Data Security and Efficient Data Access Control for Cloud data Storage Using Immediate Revocable Timestamp Multi-authority-ABE scheme". The analysis of security represents that the proposed scheme satisfies similar under adaptive chosen plaintext-attack by using Diffie-Hellman problem. Compared with the other schemes present, the proposed scheme is more economical in computational cost and storage. The timestamp is used in multi authority attributed encryption and the data user can able to view the file within the particular period of time.

Keywords: Revocable, multi-authority attribute-based encryption, timestamp, cloud data storage, elliptic-curve cryptography, Plaintext-attack

REFERENCES

[1] Yang Ming, Baokang HE and Chenhao Wang, "Efficient Revocable Multi-Authority Attributed based Encryption for cloud storage" Chang'an University Mar 2021.
[2] K. Fan, T. Liu, Y. Yang and K. Zhang, H. Li, ''A secure and efficient outsourced computation on data sharing scheme for privacy computing,'' J. Parallel Distrib. Comput., vol. 135, pp. 169–176, Jan. 2020.
[3] K. Sethi, P. Bera and A. Pradhan, ''Practical traceable multi-authority CP-ABE with outsourcing decryption and access policy updation,'' J. Inf. Secur. Appl., vol. 51, Apr. 2020, Art. no. 102435.
[4] Q. Xu, C. Tan, W. Zhu, Y. Xiao, F. Cheng and Z. Fan,''Decentralized attribute-based conjunctive keyword search scheme with online/offline encryption and outsource decryption for cloud computing,'' Future Gener. Comput. Syst., vol. 97, pp. 306–326, Aug. 2019.
[5] S. Ding, H. Liand C. Li, ''A novel efficient pairing-free CP-ABE based on elliptic curve cryptography for IoT,'' IEEE Access, vol. 6, pp. 27336–27345, May 2018.
[6] Z. Liu, Z. L. Jiang, S. M. Yiu and X. Wang, ''Practical attribute-based encryption: Outsourcing decryption, attribute revocation and policy updating,'' J. Newt. Compute. Appl., vol. 108, pp. 112–123, Apr. 2018.
[7] M. Chase, ''Multi-authority attribute-based encryption,'' in Proc. Theory Cryptogr. Conf. Berlin, Germany: Springer, Feb. 2007, pp. 515–534.
[8] J. Li, W. Yao, Y. Zhang, J. Han and J. Shen, ''User collision avoidance CP-ABE with efficient attribute revocation for cloud storage,'' IEEE Syst. J., vol. 12, no. 2, pp. 1767–1777, Jun. 2018.