IJARSCT

ISSN (Online) 2581-9429

IJARSCT

Impact Factor: 7.301

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

Volume 3, Issue 4, April 2023

Crypt Cloud: Secure and Expressive Data access by CP-ABE

Dr. S. Adinarayana[1], M Venkata Sai Pavan Kumar[2], Malluri Ramya[3],
M Gowtham Krishna Sai[4], L Durga Prasad[5]
Professor, Department of Computer Science and Engineering[1]
Students, Department of Computer Science and Engineering[2,3,4,5]
Raghu Institute of Technology, Visakhapatnam, AP, India

Abstract: *Secure distributed storage, a new cloud management, is designed to give cloud clients with out-of-control data flexible access to information while maintaining the confidentiality of redistributed data. Ciphertext-Policy Attribute-Based Encryption (CP-ABE) is regarded as one of the most promising methods for confirming the administration's security. Nevertheless, the inherent "win or bust" decoding feature of CP-ABE may result in an unavoidable security breach known as the abuse of access certification (such as unscrambling rights). In this paper, we research the two major cases of access capability misuse: One is in favor of cloud client, while the other is on the semi-trusted specialist side. To direct the maltreatment, we propose the vitally mindful master and revocable CP-ABE based circulated capacity system with white-box obviousness and auditing, insinuated as CryptCloud+. We also talk about the security investigation and use of our framework in real-world situations.*

Keywords: CP-ABE, Crypt Cloud, Data Accessing, ABE, CryptCloud+

REFERENCES

[1]. Mazhar Ali, Revathi Dhamotharan, Eraj Khan, Samee U. Khan,Athanasios V. Vasilakos, Keqin Li, and Albert Y. Zomaya. Sedasc:Secure data sharing in clouds. IEEE Systems Journal, 11(2):395–404,2017.

[2]. Mazhar Ali, Samee U. Khan, and Athanasios V. Vasilakos. Securityin cloud computing: Opportunities and challenges. Inf. Sci.,305:357–383, 2015.

[3]. Michael Armbrust, Armando Fox, Rean Griffith, Anthony DJoseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patterson,Ariel Rabkin, Ion Stoica, et al. A view of cloud computingCommunications of the ACM, 53(4):50–58, 2010.

[4]. NuttapongAttrapadung and Hideki Imai. Attribute-based encryptionsupporting direct/indirect revocation modes. In Cryptographyand Coding, pages 278–300. Springer, 2009.

[5]. Amos Beimel. Secure schemes for secret sharing and key distribution.PhD thesis, PhD thesis, Israel Institute of Technology, Technion,Haifa, Israel, 1996.

[6]. Mihir Bellare and Oded Goldreich. On defining proofs of knowledge.In Advances in Cryptology-CRYPTO'92, pages 390–420.Springer, 1993.

[7]. Dan Boneh and Xavier Boyen. Short signatures without randomoracles. In EUROCRYPT - 2004, pages 56–73, 2004.

[8]. Hongming Cai, Boyi Xu, Lihong Jiang, and Athanasios V. Vasilakos.Iot-based big data storage systems in cloud computing:Perspectives and challenges. IEEE Internet of Things Journal,4(1):75–87, 2017.

[9]. Jie Chen, Romain Gay, and Hoeteck Wee. Improved dual systemABE in prime-order groups via predicate encodings. In Advancesin Cryptology - EUROCRYPT 2015, pages 595–624, 2015.

[10]. Angelo De Caro and Vincenzo Iovino. jpbc: Java pairing basedcryptography. In ISCC 2011, pages 850–855. IEEE, 2011.

[11]. Hua Deng, Qianhong Wu, Bo Qin, Jian Mao, Xiao Liu, Lei Zhang,and Wenchang Shi. Who is touching my cloud. In ComputerSecurity-ESORICS 2014, pages 362–379. Springer, 2014.

DOI: 10.48175/IJARSCT-9257

[12]. Zhangjie Fu, Fengxiao Huang, Xingming Sun, Athanasios Vasilakos,and Ching-Nung Yang. Enabling semantic search basedon conceptual graphs over encrypted outsourced data. IEEETransactions on Services Computing, 2016.

[13]. Vipul Goyal. Reducing trust in the PKG in identity based cryptosystems.In Advances in Cryptology-CRYPTO 2007, pages 430–447.Springer, 2007.

[14]. Vipul Goyal, Steve Lu, Amit Sahai, and Brent Waters. Black-boxaccountable authority identity-based encryption. In Proceedings ofthe 15th ACM conference on Computer and communications security,pages 427–436. ACM, 2008.

[15]. Vipul Goyal, Omkant Pandey, Amit Sahai, and Brent Waters.Attribute-based encryption for fine-grained access control of encrypteddata. In Proceedings of the 13th ACM conference on Computerand communications security, pages 89–98. ACM, 2006.

[16]. Qi Jing, Athanasios V. Vasilakos, Jiafu Wan, Jingwei Lu, andDechaoQiu. Security of the internet of things: perspectives andchallenges. Wireless Networks, 20(8):2481–2501, 2014.

[17]. Allison Lewko. Tools for simulating features of composite orderbilinear groups in the prime order setting. In Advances inCryptology–EUROCRYPT 2012, pages 318–335. Springer, 2012.

DOI: 10.48175/IJARSCT-9257