6 结论与展望

云存储部署方便、价格低廉,向用户提供“数据存储即服务(DaaS)”,个人或企业用户能够高效地实现资源共享、降低成本并提高可扩展性.然而,云用户缺乏对数据的绝对控制权,数据安全,尤其是机密数据的安全,成为一大隐患,也是当前云存储中私有数据存储业务较低的根本原因之一.因此,本文提出了一种保护机密数据的分布式安全云存储机制,利用用户特征、云存储容器特征,基于多维球面原理,设计了一种分布式(K,n)门限秘密共享方案.用户将原始秘密转换 m 维球体的球心,结合云存储容器 ID 信息,进而转换成 n 个 m 维球面坐标,形成 n 个影子秘密信息,并将这些影子秘密作为机密数据分布式存储在 n 个云存储容器中.同样,云用户通过在 n 个存储容器中选取 $k(k=m+1)$个 m 维球面坐标,在线性方程组系数矩阵为满秩的情况下恢复出球心坐标,进而恢复出原始秘密信息.在分发和恢复过程中,本文设计了面向假数据攻击、共谋攻击的验证方法,同时,本文所提出的方案不需要云服务器专门存储密钥,解密密钥信息由云租户本身掌握,其密钥信息由分发者标识 ID_0、分发者持有的私有坐标 PRI 以及门限值 K 组成,这一特征加强了用户对云数据的控制能力.算法性能分析和真实验分析结果表明,本文所提出的方案是正确且有效的.

该方案在秘密重构过程中,所选取影子秘密坐标在算法逻辑上仍然存在 k 个 m 维坐标线性相关的情况,我们当前的解决方案是在重新选取 1 个影子秘密替换 k 中的任意一个坐标进行系数矩阵满秩的判断.因此在下一步的工作中,我们将进一步就如何确保秘密重构过程中系数矩阵满秩进行深入研究.同时,当前方案主要面向云租户私有业务的小文件“短”机密数据,如何将方案扩展到公有业务的大文件“长”普通数据的存储,并且保证其存储性能,也将是后续研究的重点.

致谢 谨在此对评审专家的辛勤工作、客观点评以及在论文陈述方式上给予的中肯建议表示感激.

References:

[1] Lin C, Su WB, Meng K, Liu Q, Liu WD. Cloud computing security: Architecture, mechanism and modeling. Chinese Journal of Computers, 2013,36(9):1765−1784 (in Chinese with English abstract). http://cjc.ict.ac.cn/qwjs/view.asp?id=3917 [doi: 10.3724/SP.J.1016.2013.01765]

[2] Tan S, Jia Y, Han WH. Research and development of provable data integrity in cloud storage. Chinese Journal of Computers, 2014, 37(32):1−16 (in Chinese with English abstract). http://cjc.ict.ac.cn/online/bfpub/tshang-2014821165322.pdf [doi: 10.3724/SP.J.1016.2015.00164]

[3] SNIA. Cloud data management interface (CDMITM). Version 1.1.0, 2014. http://www.snia.org/cdmi

[4] EMC (twinstrata). 2014. http://www.twinstrata.com/

[5] http://blogs.idc.com/ie/?p=730

[6] Data breach investigations report. 2014. http://www.verizonenterprise.com/

[7] Subashini S, Kavitha V. A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications, 2011,34(1):1−11. [doi: 10.1016/j.jnca.2010.07.006]

[8] Tse DWK, Chen DQ, Liu QS, Wang F, Wei ZY. Emerging issues in cloud storage security: Encryption, key management, data redundancy, trust mechanism. In: Proc. of the Int’l Conf. of Multidisciplinary Social Networks Research (MISNC 2014). CCIS 473, Springer-Verlag, 2014. 297−310. [doi: 10.1007/978-3-662-45071-0_24]

[9] Lin H, Tzeng W. A secure erasure code-based cloud storage system with secure data forwarding. IEEE Trans. on Parallel and Distributed Systems, 2012,23(6):995−1003. [doi: 10.1109/TPDS.2011.252]

[10] Abu-Libdeh H, Princehouse L, Weatherspoon H. RACS: A case for cloud storage diversity. In: Proc. of the 1st ACM Symp. on Cloud Computing (SoCC 2010). ACM Press, 2010. 1−12. [doi: 10.1145/1807128.1807165]

[11] Rabin MO. Efficient dispersal of information for security, load balancing, and fault tolerance. Journal of the ACM, 1989,36(2): 335−348. [doi: 10.1145/62044.62050]

[12] Bowers KD, Juels A, Oprea A. HAIL: A high-availability and integrity layer for cloud storage. In: Proc. of the 16th ACM Conf. on Computer and Communications Security (CCS 2009). ACM Press, 2009. 187−198. [doi: 10.1145/1653662.1653686]

[13] Resch JK, Plank JS. AONT-RS: Blending security and performance in dispersed storage systems. In: Proc. of the 9th USENIX Conf. on File and Storage Technologies (FAST 2011). San Jose, 2011. 191−202. http://static.usenix.org/legacy/events/fast11/tech/full_papers/Resch.pdf

[14] Xiong H, Zhang X, Yao D, Wu X, Wen Y. Towards end-to-end secure content storage and delivery with public cloud. In: Proc. of the 2nd ACM Conf. on Data and Application Security and Privacy. ACM Press, 2012. 257−266. [doi: 10.1145/2133601.2133633]

[15] Kikuchi H, Itoh K, Ushida M, Yamaoka Y, Oikawa T. Secret sharing scheme with efficient keyword search for cloud storage. In: Proc. of the 9th Asia Joint Conf. on Information Security. IEEE Press, 2014. 164−169. [doi: 10.1109/AsiaJCIS.2014.33]

[16] Alsolami F, Boult T. CloudStash: Using secret-sharing scheme to secure data, not keys, in multi-clouds. In: Proc. of the 11th Int'l Conf. on Information Technology: New Generations (ITNG 2014). IEEE Press, 2014. 315−320. [doi: 10.1109/ITNG.2014.119]

[17] Fu YX, Luo SM, Shu JW. Survey of secure cloud storage system and key technologies. Journal of Computer Research and Development, 2013,50(1):136−145 (in Chinese with English abstract). http://crad.ict.ac.cn/CN/Y2013/V50/I1/136

[18] Grossman RL, Gu Y, Sabala M, Zhang WZ. Compute and storage clouds using wide are high performance networks. Future Generation Computer Systems, 2009,25(2):179−183. [doi: 10.1016/j.future.2008.07.009]

[19] Cao N, Wang C, Li M, Ren K, Lou W. Privacy-Preserving multi-keyword ranked search over encrypted cloud data. IEEE Trans. on Parallel and Distributed Systems, 2014,25(1):222−233. [doi: 10.1109/TPDS.2013.45]

[20] Zhang XY, Liu C, Nepal S, Pandey S, Chen JJ. A privacy leakage upper bound constraint-based approach for cost-effective privacy preserving of intermediate data sets in cloud. IEEE Trans. on Parallel and Distributed Systems, 2013,24(6):1192−1202. [doi: 10.1109/TPDS.2012.238]

[21] Roy I, Setty STV, Kilzer A, Shmatikov V, Witchel E. Airavat: Security and privacy for mapreduce. In: Proc. of the 7th USENIX Conf. on Networked Systems Design and Implementation (NSDI 2010). ACM Press, 2010. 20. https://www.usenix.org/legacy/event/nsdi10/tech/full_papers/roy.pdf

[22] Puttaswamy KPN, Kruegel C, Zhao BY. Silverline: Toward data confidentiality in storage-intensive cloud applications. In: Proc. of the 2nd ACM Symp. on Cloud Computing (SoCC 2011). ACM Press, 2011. 1−13. [doi: 10.1145/2038916.2038926]

[23] Bessani A, Correia M, Quaresma B, André F, Sousa P. DepSky: Dependable and secure storage in a cloud-of-clouds. In: Proc. of the 6th Conf. on Computer Systems. ACM Press, 2011. 31−46. [doi: 10.1145/1966445.1966449]

[24] Cachin C, Haas R, Vukolic M. Dependable storage in the intercloud. IBM Research Report, 2010. http://domino.research.ibm.com/library/cyberdig.nsf/papers/630549C46339936C852577C200291E78/$File/rz3783.pdf

[25] Chor B, Goldwasser S, Micali S, Awerbuch B. Verifiable secret sharing and achieving simultaneity in the presence of faults. In: Proc. of the Foundations of Computer Science. IEEE, 1985. 383−395. [doi: 10.1109/SFCS.1985.64]

[26] Pedersen TP. Non-Interactive and information-theoretic secure verifiable secret sharing. In: Proc. of the Advances in Cryptology—CRYPTO'91. Berlin, Heidelberg: Springer-Verlag, 1992. 129−140. [doi: 10.1007/3-540-46766-1_9]

[27] Gennaro R, Rabin MO, Rabin T. Simplified VSS and fast-track multiparty computations with applications to threshold cryptography. In: Proc. of the 17th Annual ACM Symp. on Principles of Distributed Computing. ACM Press, 1998. 101−111. http://www.eecs.harvard.edu/~cat/cs/tlc/papers/grr.pdf

[28] Herzberg A, Jarecki S, Hugo K, Yung M. Proactive secret sharing or: How to cope with perpetual leakage. In: Proc. of the 15th Annual Int'l Cryptology Conf. on Advances in Cryptology. Springer-Verlag, 1998. 339−352. [doi: 10.1007/3-540-44750-4_27]

[29] Tan ZH, Yang GM, Cheng W, Wang XW. Distributed secret sharing scheme based on personalized spherical coordinates space. Computer Science and Information Systems, 2013,10(3):1269−1291. [doi: 10.2298/CSIS120801048T]

[30] Harn L. Efficient sharing (broadcasting) of multiple secrets. IEEE Proc. of Computers and Digital Techniques, 1995,142(3):237−240. [doi: 10.1049/ip-cdt:19951874]

[31] Tang CM, Wu DO, Chronopoulos AT, Raghavendra CS. Efficient multi-party digital signature using adaptive secret sharing for low-power devices in wireless networks. IEEE Trans. on Wireless Communications, 2009,8(2):882−889. [doi: 10.1109/TWC.2008.071286]

[32] Kamara S, Lauter K. Cryptographic cloud storage. In: Proc. of the Financial Cryptography and Data Security. LNCS 6054, Springer-Verlag, 2010. 136−149. [doi: 10.1007/978-3-642-14992-4_13]

[33] Popa RA, Lorch JR, Molnar D, Wang HJ, Zhuang L. Enabling security in cloud storage SLAs with CloudProof. In: Proc. of the USENIX ATC. ACM Press, 2011. 1−12. http://www.mit.edu/~ralucap/cloudproof.pdf

[34] Kumbhare A, Simmhan Y, Prasanna V. Cryptonite: A secure and performant data repository on public clouds. In: Proc. of the 5th Int'l Conf. on Cloud Computing. IEEE Press, 2012. 510−517. [doi: 10.1109/CLOUD.2012.109]

[35] Alsolami F, Chow CE. *N*-Cloud: Improving performance and security in cloud storage. In: Proc. of IEEE the 14th Int'l Conf. on High Performance Switching and Routing (HPSR). IEEE Press, 2013. 221−222. [doi: 10.1109/HPSR.2013.6602319]

[36] Zissis D, Lekkas D. Addressing cloud computing security issues. Future Generation Computer Systems, 2012,28(3):583−592. [doi: 10.1016/j.future.2010.12.006]

[37] Shamir A. How to share a secret. Communications of the ACM, 1979,22(11):612−613. [doi: 10.1145/359168.359176]

[38] Blakley GR. Safeguarding cryptographic keys. In: Proc. of the National Computer Conf. 1979. 313−317. http://www.computer.org/csdl/proceedings/afips/1979/5087/00/50870313.pdf

[39] Tompa M, Woll H. How to share a secret with cheaters. Journal of Cryptology, 1989,1(3):133−138. [doi: 10.1007/BF02252871]

[40] Bj¨orkqvist M, Cachin C, Haas R, Hu XY, Kurmus A, Pawlitzek R, Vukolić M. Design and implementation of a key-lifecycle management system. Lecture Notes in Computer Science, 2010,6052:160−174. [doi: 10.1007/978-3-642-14577-3_14]

[41] AlZain MA, Soh B, Pardede E. MCDB: Using multi-clouds to ensure security in cloud computing. In: Proc. of the 9th Int'l Conf. on Dependable, Autonomic and Secure Computing (DASC 2011). IEEE Press, 2011. 784−791. [doi: 10.1109/DASC.2011.133]

[42] Chervyakov NI, Babenko MG, Deryabin MA, Nazarov AS. Cryptanalysis of secret sharing schemes based on spherical spaces. In: Proc. of the 8th Int'l Conf. on Application of Information and Communication Technologies (AICT). IEEE Press, 2014. 1−5. [doi: 10.1109/ICAICT.2014.7035900]

附中文参考文献:

[1] 林闯,苏文博,孟坤,刘渠,刘卫东.云计算安全:架构、机制与模型评价.计算机学报,2013,36(9):1765−1784. http://cjc.ict.ac.cn/qwjs/view.asp?id=3917 [doi: 10.3724/SP.J.1016.2013.01765]

[2] 谭霜,贾焰,韩伟红.云存储中的数据完整性证明研究及进展.计算机学报,2014,37(32):1−16. http://cjc.ict.ac.cn/online/bfpub/tshang-2014821165322.pdf [doi: 10.3724/SP.J.1016.2015.00164]

[17] 傅颖勋,罗圣美,舒继武.安全云存储系统与关键技术综述.计算机研究与发展,2013,50(1):136−145. http://crad.ict.ac.cn/CN/Y2013/V50/I1/136

谭振华(1980－),男,湖南双峰人,博士,副教授,CCF 专业会员,主要研究领域为分布式网络安全,门限密码学,云安全.

程维(1970－),男,副教授,主要研究领域为复杂网络,信息安全.

杨广明(1961－),男,教授,主要研究领域为网络安全,密码学.

宁婧宇(1990－),女,硕士生,主要研究领域为门限密码学.

王兴伟(1968－),男,博士,教授,博士生导师,CCF 高级会员,主要研究领域为未来互联网,云计算,网络空间安全.