SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

ブロックチェーンを用いた重複データ排除機能付き マルチクラウドストレージ監査方式

Deduplicatable Multi-Cloud Storage Data Auditing Scheme Using Blockchain

廣友 雅徳 * Masanori Hirotomo
嘉戸 裕一 † Yuichi Kato
白石 善明 † Yoshiaki Shiraishi
今村 光良 ‡ Imamura Mitsuyoshi
森井 昌克 † Masakatu Morii

キーワード クラウドストレージ，監査，ブロックチェーン，スマートコントラクト

あらまし

ネットワークストレージサービスはストレージシステムの安全性，信頼性，スケーラビリティを解決する手段であり，現在広く普及している．クラウドストレージサービスにおいてデータ監査は重要な課題と考えられており，その解決法として PDP（Provable Data Possession）は有効である [1, 2]．近年，ブロックチェーン技術の応用について様々な研究がなされており，クラウドストレージの PDP 監査への応用が提案されている [3, 4]．また，ブロックチェーン技術を応用したクラウドストレージ監査方式として，クラウドストレージの効率利用を目的とした重複データ排除機能 [5] や，方式の安全性の根拠に第三者監査機関と必要しない方式 [6] が提案されている．さらには，クラウドストレージサービスを多重化に拡張したマルチクラウド監査方式が提案されている [7, 8]．特に，文献 [8] の方式はブロックチェーン技術のスマートコントラクトを用いることによって第三者監査機関を必要としないマルチクラウド監査方式を実現している．

本稿では，第三者監査機関を必要としない重複データ排除機能付きマルチクラウドストレージ監査方式を提案する．提案方式では，第三者監査機関を用いず，ブロックチェーン技術の一つであるスマートコントラクトによってストレージ監査機能，重複データ排除機能を実現している．さらに，第三者監査機関の存在やクラウドサービスの正常な動作を仮定とせず，その不正な動作をスマートコントラクトによる異議仲裁機能によって検出可能としている．

* 佐賀大学 Saga University
† 神戸大学 Kobe University
‡ 野村アセットマネジメント株式会社 Nomura Asset Management Co., Ltd

参考文献

[1] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, “Provable data possession at untrusted stores,” Proc. 14th ACM Conf. Comput. Commun. Security, pp.598—609, 2007.

[2] S. Shin and T. Kwon, “A survey of public provable data possession schemes with batch verification in cloud storage,” J. Internet Serv. Inf. Security (JISIS), vol.5, no.3, pp.37—47, 2015.

[3] J. Xue, C. Xu, J. Zhao, and J. Ma,“Identity-based public auditing for cloud storage systems against malicious auditors via blockchain,” Science China Information Sciences, vol.62, no.3, p.32104, 2019.

[4] Y. Zhang, C. Xu, X. Lin, and X. S. Shen, “Blockchain-based public integrity verification for cloud storage against procrastinating auditors,” IEEE Trans. Cloud Comput., pp.1—15, 2019.

[5] Y. Xu, C. Zhang, G. Wang, Z. Qin, and Q. Zeng, “A blockchain-enabled deduplicatable data auditing mechanism for network storage services,” IEEE Trans. Emerg. Topics Comput.,, vol.9, no.3, pp.1421–1432, 2020.

[6] Y. Xu, J. Ren, Y. Zhang, C. Zhang, B. Shen, and Y. Zhang, “Blockchain empowered arbitrable data auditing scheme for network storage as a service,” IEEE Trans. Serv. Comput.., vol.13, no.2, pp.289–300, 2020.

[7] X. Yang, X. Pei, M. Wang, T. Li, and C. Wang, “Multi-replica and multi-cloud data public audit scheme based on blockchain,” IEEE Access, vol.8, pp.144 809—144 822, 2020.

[8] C. Zhang, Y. Xu, Y. Hu, J. Wu, J. Ren, and Y. Zhang, “A blockchain- based multi-cloud storage data auditing scheme to locate faults” IEEE Tran. Cloud Computing (Early Access).