

Enhancing Privacy and Security in Distributed Data Sharing through Re-Encryption

Komal Varpe¹, Shraddha Umbarkar², Rohit Kalekar³, Shashank Singh Rajawat⁴, K. S. Mulani⁵

Department of Computer Engineering^{1,2,3,4,5}
Sinhgad Institute of Technology, Lonavala, India

Abstract: *Data sharing in cloud computing is a valuable application, but data security remains a concern. To address this, we propose a proxy re-encryption method for secure data transfer in the cloud. Using identity-based encryption, data owners can send encrypted data to the cloud, while authorized users can access it through proxy re-encryption. In IoT environments, an edge device acts as a proxy server, performing complex calculations due to limited device capacity. Leveraging information-centric networking, we enhance service quality and network bandwidth by efficiently utilizing cached data in the proxy. Our system is built on blockchain technology, enabling decentralized data sharing, improving centralized systems' effectiveness, and enabling fine-grained data access management. Through a security study and evaluation, our system offers privacy protection, authenticity, and reliability.*

Keywords: Role-based Access Control (RBAC), Blockchain, Cryptography, Decentralized, Distributed Systems, Cloud Storage

REFERENCES

- [1] J. Yu, K. Wang, D. Zeng, C. Zhu, and S. Guo, "preserving data aggregation computing in cyber-physical social systems," *ACM Transactions on Cyber-Physical Systems*, vol. 3, no. 1, p. 8, 2019.
- [2] H. Ren, H. Li, Y. Dai, K. Yang, and X. Lin, in internet of things with privacy preserving: Challenges, solutions and opportunities," *IEEE Network*, vol. 32, no. 6, pp. 144151, 2019.
- [3] J. Li, H. Ye, W. Wang, W. Lou, Y. T. Hou, J. Liu, and R. Lu, Efficient and secure outsourcing of differentially private data publication," in *Proc. ESORICS*, 2019, pp. 187-206.
- [4] Xu, Jinliang, et al Edgence: A blockchain-enabled edge-computing platform for intelligent IoTbased Apps. *China Communications* 17.4 (2020): 78-87.
- [5] Huang, Zheng, Zeyu Mi, and Zhichao Hua. HCloud: A trusted JointCloud serverless platform for IoT systems with blockchain. *China Communications* 17.9 (2020): 1-10.
- [6] Gheitanchi, Shahin. Gamified service exchange platform on blockchain for IoT business agility 2020 *IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*. IEEE, 2020.
- [7] G. Xu, H. Li, Y. Dai, K. Yang, and X. Lin, efficient and geometric range query with access control over encrypted spatial data," *IEEE Trans. Information Forensics and Security*, vol. 14, no. 4, pp. 870885, 2019.
- [8] K. Yang, K. Zhang, X. Jia, M. A. Hasan, and X. Shen, Privacy preserving attribute- keyword based data publish-subscribe service on cloud platforms," *Information Sciences*, vol. 387, pp. 116-131, 2017.
- [9] Choi, Jungyong, et al. "Random Seed Generation For IoT Key Generation and Key Management System Using Blockchain." 2020 *International Conference on Information Networking (ICOIN)*. IEEE, 2020.
- [10] "Data sharing in cloud computing using blockchain and re-encryption." by S. Chaudhary, P. Kumar, and V. Tyagi. *Future Generation Computer Systems* 112 (2020): 441-452.