Secure and Privacy-Preserving Data Sharing in Multi-Cloud Environments: A Blockchain-Based Approach

- Pham Thi Ngoc Diep, Faculty of Information Technology, University of Science, Vietnam National University, Ho Chi Minh City, Vietnam

The increasing adoption of cloud computing has led to the proliferation of multi-cloud environments, where organizations leverage services from multiple cloud providers to achieve better reliability, flexibility, and cost-efficiency. However, data sharing across different cloud platforms introduces significant security and privacy challenges, as sensitive information may be exposed to unauthorized parties or vulnerable to attacks. This research paper presents a novel blockchain-based approach to enable secure and privacy-preserving data sharing in multi-cloud environments. By leveraging the decentralized and immutable nature of blockchain technology, the proposed framework ensures data integrity, confidentiality, and auditability throughout the data sharing process. The research methodology involves the design and implementation of a permissioned blockchain network that acts as a secure and transparent layer for data sharing among multiple cloud providers. The framework incorporates advanced cryptographic techniques, such as homomorphic encryption and secure multi-party computation, to protect sensitive data while allowing authorized parties to perform computations on encrypted data without revealing the underlying information. The proposed approach is evaluated through rigorous security analysis and performance benchmarking, demonstrating its effectiveness in preventing data breaches, unauthorized access, and privacy leaks. The study also presents a detailed analysis of the scalability and efficiency of the blockchain-based data sharing framework, considering factors such as transaction throughput, latency, and storage overhead. The findings of this research have significant implications for organizations operating in multi-cloud environments, enabling them to securely share and collaborate on sensitive data across different cloud platforms. By leveraging blockchain technology, the proposed approach provides a transparent and tamper-proof mechanism for data sharing, enhancing trust and accountability among participating entities. This research contributes to the advancement of secure and privacy-preserving data sharing solutions in the era of multi-cloud computing, addressing the critical challenges of data protection and compliance in complex cloud ecosystems.

References

[1] K. Alwasel, Y. Li, P. P. Jayaraman, S. Garg, R. N. Calheiros, and R. Ranjan, “Programming SDN-native big data applications: Research gap analysis,” *IEEE Cloud Comput.*, vol. 4, no. 5, pp. 62–71, Sep. 2017.

[2] M. Abouelyazid, “Forecasting Resource Usage in Cloud Environments Using Temporal Convolutional Networks,” *Applied Research in Artificial Intelligence and Cloud Computing*, vol. 5, no. 1, pp. 179–194, Nov. 2022.

[3] M. Yousif, “Cloud-native applications—the journey continues,” *IEEE Cloud Comput.*, vol. 4, no. 5, pp. 4–5, Sep. 2017.

[4] M. Abouelyazid and C. Xiang, “Architectures for AI Integration in Next-Generation Cloud Infrastructure, Development, Security, and Management,” *International Journal of Information and Cybersecurity*, vol. 3, no. 1, pp. 1–19, Jan. 2019.