Decentralized Cloud Resource Access Control using Multi-Signature Smart Contracts with Threshold Cryptography [BlockChains]

Ravi Teja Gandu
x24112490
Programme Code - Research in Computing CA1
National College of Ireland

1 Research Problem Background

Cloud computing has revolutionized the management of organizations, and its revenue in the world was estimated to be $247.7 billion in 2024. Older centralized access control systems represent a security risk, which is why the Identity and Access Management (IAM) market is predicted to reach $22.9 billion by 2024. Multi-signature smart contracts may be an attractive way to address them because they spread access control decisions among many parties, removing single points of failure that are inherent to centralized systems. The threshold cryptography protocols have recently been practical, with signature generation times below a second and allowing flexible threshold choices (Komlo & Goldberg 2020). However, its application in modern systems has severe drawbacks in public cloud settings because the existing multi-signature schemes are optimized to be used in the context of cryptocurrencies rather than cloud resource management, and the compatibility with the public cloud APIs demands innovative architectural solutions that are not studied systematically yet. Recent studies in the area of gas optimization strategies show that the smart contract efficiency can be enhanced by up to 40 percent via optimized data storage and conditional statements (Porkodi & Kesavaraja 2024). Blockchain-based decentralized access control systems mitigate numerous shortcomings of the centralized systems. It is estimated that the blockchain identity management market will expand greatly in the future, which means that the industry takes great interest in decentralized solutions. Nonetheless, major issues are still present, including the fact that current blockchain systems can only handle 7-30 transactions per second whereas traditional systems can process more than 2,000 TPS, and the scalability bottlenecks prevent a practical use in large-scale cloud settings (Yang et al. 2020).

2 Research Question

What are the measurable security and performance benefits achieved through the implementation of multi-signature smart contract architecture with adaptive threshold cryptography on the resilience of access control, authentication latency, gas usage efficiency, and scalability of systems in the public cloud resource management systems as opposed to the centralized IAM systems?

3 Justification

The proposed research will fill significant open questions in cloud security architecture, in terms of designing new smart contract frameworks dedicated and specialized in controlling public cloud resources access. Recent work shows that access control schemes built on blockchain can realize fine-grained access control with low computation overheads via proxy encryption and decryption scheme (Yan et al. 2023). The research is relevant towards enhancing the patterns of smart contract architecture, building scalable blockchain applications on enterprise clouds, and devising novel approaches to interface decentralized systems with the existing cloud infrastructure. The results of the recent benchmarking tests illustrate that FROST like threshold signature schemes can perform signature generation and signature verification in less than 1.6 milliseconds with 2048-bit security parameter (Ricci et al. 2022). With the largest public cloud providers providing full APIs to manage access, various blockchain platforms have smart contract deployment with well-established development frameworks, and threshold cryptography libraries have ready-to-use building blocks, this research is certainly possible. The experimental implementation methodology guarantees practically-oriented, quantifiable results, which could be further proved through the established performance evaluation schemes of blockchain systems in an independent manner. The study uses some measurable, cloud-specific dimensions such as the time taken to process access requests, the gas used per operation in smart contracts, the throughput of the system expressed in the number of access decisions made in a second, the latency of the API responses, and the rate of security incident detection. The study is devoted to the enhancement of cloud security and access control, which helps to ensure enhanced protection of organizational resources and user data.

4 Specific Items to Be Addressed

Item #1 The architecture and construction of gas-optimized multi-signature smart contract system composed of Solidity on Ethereum-compatible networks (Maldonado-Ruiz et al. 2025) which supports FROST threshold signature scheme consisting of modular architecture to allow threshold to be dynamically increased or decreased.

Item #2 The creation of RESTful API gateway between blockchain transactions and AWS and Azure Cloud IAM systems, identity mapping and compliance monitoring systems.

Item #3 This system should be able to perform benchmarks comprehensively on the transaction throughput, gas consumption, authentication latency and scalability based on realistic cloud access patterns at enterprise-level workloads.

Item #4 Additional forms of validation like Byzantine fault tolerance assessment, smart contract vulnerability analysis, and relative security assessment compared to the conventional centralized IAM systems via simulation-based methods have to be conducted as well.

Item #5 The experimental method should resort to the use of controlled lab testing with cloud testbeds and blockchain testnets and comparative evaluation in terms of the performance gains over current solutions.

References

Komlo, C. & Goldberg, I. (2020), Frost: Flexible round-optimized schnorr threshold signatures, *in* 'International Conference on Selected Areas in Cryptography', Springer, pp. 34–65.

Maldonado-Ruiz, D., Hwang, C. Y., Jankovskaja, E., Sadykova, K., Mazari, M., Torres, J. & El Madhoun, N. (2025), Implementation of two-signature security on an identity storage smart contract, *in* 'International Conference on Advanced Information Networking and Applications', Springer, pp. 81–94.

Porkodi, S. & Kesavaraja, D. (2024), 'Escalating gas cost optimization in smart contract', *Wireless Personal Communications* **136**(1), 35–59.

Ricci, S., Dzurenda, P., Casanova-Marqués, R. & Cika, P. (2022), Threshold signature for privacy-preserving blockchain, *in* 'International Conference on Business Process Management', Springer, pp. 100–115.

Yan, L., Ge, L., Wang, Z., Zhang, G., Xu, J. & Hu, Z. (2023), 'Access control scheme based on blockchain and attribute-based searchable encryption in cloud environment', *Journal of Cloud Computing* **12**(1), 61.

Yang, C., Tan, L., Shi, N., Xu, B., Cao, Y. & Yu, K. (2020), 'Authprivacychain: A blockchain-based access control framework with privacy protection in cloud', *Ieee Access* **8**, 70604–70615.