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

Ravi Teja Gandu

x24111490

Master of Science in Cloud Computing

Programme: Research in Computing CA2

National College of Ireland

**Abstract**

The research delves into the use of decentralized cloud resource access control through multi-signature smart contracts that are further enhanced with threshold cryptography, centered on the FROST (Flexible Round-Optimized Schnorr Threshold) signature scheme. Conventional cloud Identity and Access Management (IAM) systems are deeply centralized, leading to vulnerabilities, having single points of failure, and being coupled with limited transparency in access control decisions. By proposing this study which combines FROST threshold signatures and Ethereum gas-optimized Solidity smart contracts, we employ a Byzantine fault-tolerant access control system for multi-cloud environments. This project intends to show the benefits in security gained through decentralized consensus, the cut in operational costs coming from gas optimization, and the sustainment of performance at enterprise level with below subsecond authorization time. The project is a step forward in the path towards semiautonomous IAM systems built on the basis of blockchain using FROST threshold signature with cloud-native access control.

**Keywords:** FROST threshold cryptography, blockchain IAM, multi-signature smart contracts, Byzantine fault tolerance

# Introduction

Centralized IAM systems, while being understood as close to mature, have certain built-in weaknesses, such as breaking points, insider threats, and inadequate transparency in access control decisions (Punia et al., 2024). The use of blockchain technology gives a total transformation in tackling these questions through decentralized agreement protocols as well as cryptographic security logical databases. The contemporary breakthroughs in the field of threshold cryptography, with particular reference to FROST signature scheme, enable it to be implemented practically without compromising the traditional performance (Connolly et al., 2024). The FROST algorithm tests network resources through many rounds, saving the required ones by cutting the rounds to two without downgrading security to forgery. Bottom line, it can be deployed in businesses that have high demands on speed and throughput. Integrating ideas, recent advancements in contract optimization have solved the previous blockchain scalability concerns, storage packing techniques gaining 20-30% gas and assembly optimization techniques providing similar results (Nelaturu et al., 2021). The symbiotic relationship of the aforementioned technologies generates the chance of reimagining the access control of cloud technologies. Utilizing the FROST threshold signatures and Solidity smart contracts with gas optimization for decentralized IAM is now possible for organizations that previously were prone to centralized vulnerabilities while blocking them.

***Problem Statement:*** Centralized credentials can be seen as a common failure, for example, numerous breaches where administrative credentials were exposed resulting in security incidents on a company-wide scale. Additionally, traditional IAM systems are disposed to faulty access control decisions that lead to difficulties in budget audits, as the authorization logic is unobvious, and the detection of anomalous behaviors is usually too late. Multi-cloud configurations, on the other side, make the situation more difficult by adding the identity federation issue that is present among providers. The constraint of performance on actual blockchain-based IAM applications has been the reason as to why their adoption has not increased even though they contain security advantages. The Ethereum blockchain was not the best choice for early applications due to the very high gas fees that were required, for example, multi-signature operations that consumed 80,000-120,000 gas units per transaction. In times of high network traffic, transaction fees increased beyond $100, thus making blockchain purchasing impossible. Furthermore, the consensus finality times of 12-15 seconds on public blockchains have not met the enterprise requirements of less than one second authorization responses degrading the system performance.

***Motivation:*** The need for cloud security improvement is a key reason for doing this research at a time when cyber threats are constantly on the rise. The solution for these are blockchains which can impose immutable authorization logs for purposes of forensic discovery as well as compliance provisions and thus meet the increasing regulatory requests for data protection and access control transparency. Moreover, studies point towards the decentralization of IAM as cost-effective solution. In fact, automation of routine tasks through the use of smart contracts like this can lead to this result by eliminating intermediaries and by automating policy enforcement. The potential of gas optimization techniques, especially those generated for IFC applications, stands for a 50-75% financial success in comparison with ordinary implementations, which indicates that the usage of blockchain in security management is a winning advantage (Kim and Kim, 2024). The development of the FROST standard for technical cryptography has also matured, which means there are no more barriers for the deployment of technology in practice. While previous threshold signature algorithms demanded a communication complexity of O(n²), FROST is linear and the signature size is constant irrespective of the number of participants. This is because of the new Ethereum solutions which have brought Layer 2 rollups into the picture for optimum efficiency that is needed for decentralized access control.

**Research Question.** What are the implementation benefits of FROST threshold cryptography with gas-optimized multi-signature smart contracts to create an effective Byzantine fault-tolerant access control system while contrasting it with the conventional centralized IAM solutions?

**Contributions:**

This research has made the following important advancements in the domain of decentralized IAM:

* A full-scale implementation of FROST threshold signatures, gas-optimized Solidity smart contracts, and cloud access control to achieve the lowest possible gas consumption through an innovative storage packing and assembly optimizations approach while still ensuring the required security.
* The inclusion of special consensus Layer 2 scaling strategies that support adaptive workloads while keeping under-a-second latency for authorization and implementing more than 1,000 transactions per second.
* Bringing in the BFT consensus-integrated FROST signatures through design and validation, and improving the node circulation with no loss of system up time to be devoid of coordinated attacks and network failures.
* The synchronization of the blockchain-based IAM systems through cross-cultural benchmarking methodologies, introducing metrics such as gas cost, security incident detection rates, etc., with a token of acknowledgment for the testing done using the production workloads.

This report is structured as follows: In Section 2, we provide a thorough review of the literature exploring the current developments in threshold cryptography, smart contracts, and blockchain-based IAM systems. The methodology has been clearly explained in the Section 3 which covers system architecture, implementation specifications, and evaluation plans. We shall also overview the ethic compliances and project timeline.

# Literature Review

## Threshold Cryptography and FROST Implementations

Considering threshold cryptography, the work by (Komlo and Goldberg, 2020) is important as it deals with FROST signatures. This approach greatly influenced the area by offering fewer communication rounds while still providing the same security guarantees. It unveiled a two-round threshold signature protocol that went down the network overhead from O(n²) to O(n) complexity, hence making it possible to put into practice with enormous groups of participants. The unrivaled concept of the protocol comes with preprocessing commitments that support single-round signing operations, which is the key edge for achieving company-grade performance in the access control systems.

The FROST standard adoption, as evidenced by the release of RFC 9591 (Connolly et al., 2024), is a critical turning point in the threshold cryptography mainstreaming. This document contains an IETF specification that includes five cipher suites such as Ed25519, P-256, and secp256k1, so that different blockchain platforms and cryptographic libraries can work together effectively. This standard not only sets the guidelines for implementation of distributed key generation, share refreshing, and recovery mechanisms, but also attends to the critical practical issues facing the conformity of practical implementation. Besides, the specification has a particular section on test vectors, along with security considerations that are all-encompassing for implementations across different programming languages, and platforms.

The latest extensions of FROST address the management of dynamic participants, which is a vital requirement in enterprise access control systems. (Cimatti et al., 2024) introduced Dynamic-FROST, a FROST protocol combined with CHURP (CHUrn-Robust Proactive secret sharing), allowing for the update of thresholds and participants without the use of trusted third parties. With this breakthrough, organizations are able to adjust access control rights and include or exclude signers without having to regenerate cryptographic keys, in turn removing what has generally been seen as a major disadvantage of old static threshold approaches.

The ROAST protocol is the one that is used to increase the robustness by dealing with potential security threats (Ruffing et al., 2022). The protocol is based on the wrapper approach that guarantees that all signatures will still go through even with the presence of harmful participants. This work has been proven to be scalable under configurations when tested on about a hundred participants and took less than 7 seconds for completion of the signing operations, even with the presence of 33 Byzantine nodes. This level of solidity is an absolute must for any business case out there, where the availability cannot afford failures from individual malicious ones.

## Smart Contract Optimization for Gas Efficiency

The availability of blockchain-based access control is strongly correlated with transaction costs, which makes gas optimization, a major research focus. The recent steps in Solidity optimization have managed to reduce expenses considerably through the alteration of compilers and design patterns among other factors as shown by (He et al., 2024). Using a real-world case, they were able to identify features peculiar to Solidity including mismanaged storage access, memory usage issues, and unnecessary computation which had a negative impact on contract operations.

The funds that are saved through gas optimization in access control contracts will be mostly used on features that are much more beneficial to the project as a whole. (Nelaturu et al., 2021) study on contract rewriting of the Json file format asserted a gas unit surplus of 23,943 for a single transaction through the one-time data structure alteration and subsequent access changes. The method used by them is based on formal synthesis which employs syntactic changes and upholds behavioural equivalence, a necessity for the access control logic which is security-critical.

Ethereum's evolution has unlocked both new obstacles and optimization opportunities. Although the merge did not directly impact gas fees, it paved the way for future scaling improvements, such as the proto-danksharding (EIP-4844), which has already been implemented in March 2024. Layer 2 transactions are, therefore, reduced by 90% making blockchain-based access controls economically viable for high-volume operations. The SolOSphere framework (Khanzadeh and Alafi, 2024) offers a single package for gas optimization that links parsing, deployment, verification, and analysis tools with the help of AI-assisted development capabilities.

Optimizing Assembly levels in turn also reduces latency in paths that have become relevant to the scrutiny of executions. The gas-expensive pattern detection research (Li et al., 2023) was directed by machine learning initiatives which achieved an accuracy of 83.05% in the hold of the optimization opportunities identified. The case of multi-signature verification, the hand-crafted assembly that was made of signature confirmation routines, was able to decrease gas expenses by 5-15% in comparison to the high-level Solidity, while these optimizations needed to be scrupulously vetted so that they did not impact security norms. An active field of exploration has been the balancing of optimization and auditability, with formal verification devices making progress in the support of assembly-level code exploration.

## Blockchain-Based Identity and Access Management Systems

The implementation of blockchain in IAM has given rise to a number of researches, including the systematic analysis by (Punia et al., 2024). The thorough analysis characterized twelve different blockchain-centric models for access control that include role-based (RBAC), attribute-based (ABAC), capability-based (CBAC) models, among others. Some of the most marked features are the widespread use of the smart contract in the policy enforcement area and the adoption of the hybrid model where the policy is stored on-chain, but the execution is off-chain to enhance efficiency.

Hu (2022) presented a canonical path which maps the prior working of XACML and NGAC onto blockchain architectures discussed in this research whose focus is on smart contracts and distributed nodes. It also identifies the performance disparities, one of which is the Ethereum's limitation of 14 TPS in contrast to Visa's 24,000 TPS rate and also advises on the architectural patterns to overcome the issues by means of caching, off-chain computation, and selective on-chain enforcement.

Multi-cloud identity federation is a particular challenge that has been tackled by recent research. In (Moyo and du Toit, 2024), they present the CloudBloc design, which is a federated IAM on the blockchain technology across cloud providers. This takes away the central identity provider and uses smart contracts to validate users through user base public-private key pairs held by the wallet of the user. In addition, the direct integration with a cloud service provider is more biased towards latency when relating to authentication and decentralize trust. The model can be applied and implemented in certain prototype methods with the AWS and Azure IAM.

The landmark blockchain-based IAM systems have gone through remarkable progress as new consensus mechanisms have been introduced. The ZK-BFT protocol (Li et al., 2023) includes zero-knowledge proofs and Byzantine fault tolerance, which allows for a privacy-preserving access control in permissioned networks through these undetectable proof traditional consensus weakness. ZK-BFT, a consensus protocol developed on Hyperledger Fabric and based on the Ursa cryptography library, makes sure that the integrity of the consensus is not compromised and that the authorization data is not revealed at the same time. This strategy focuses on the security conscious performance and also focuses on the privacy of an enterprise in operations that must comply with regulations such as in healthcare and finance among other businesses.

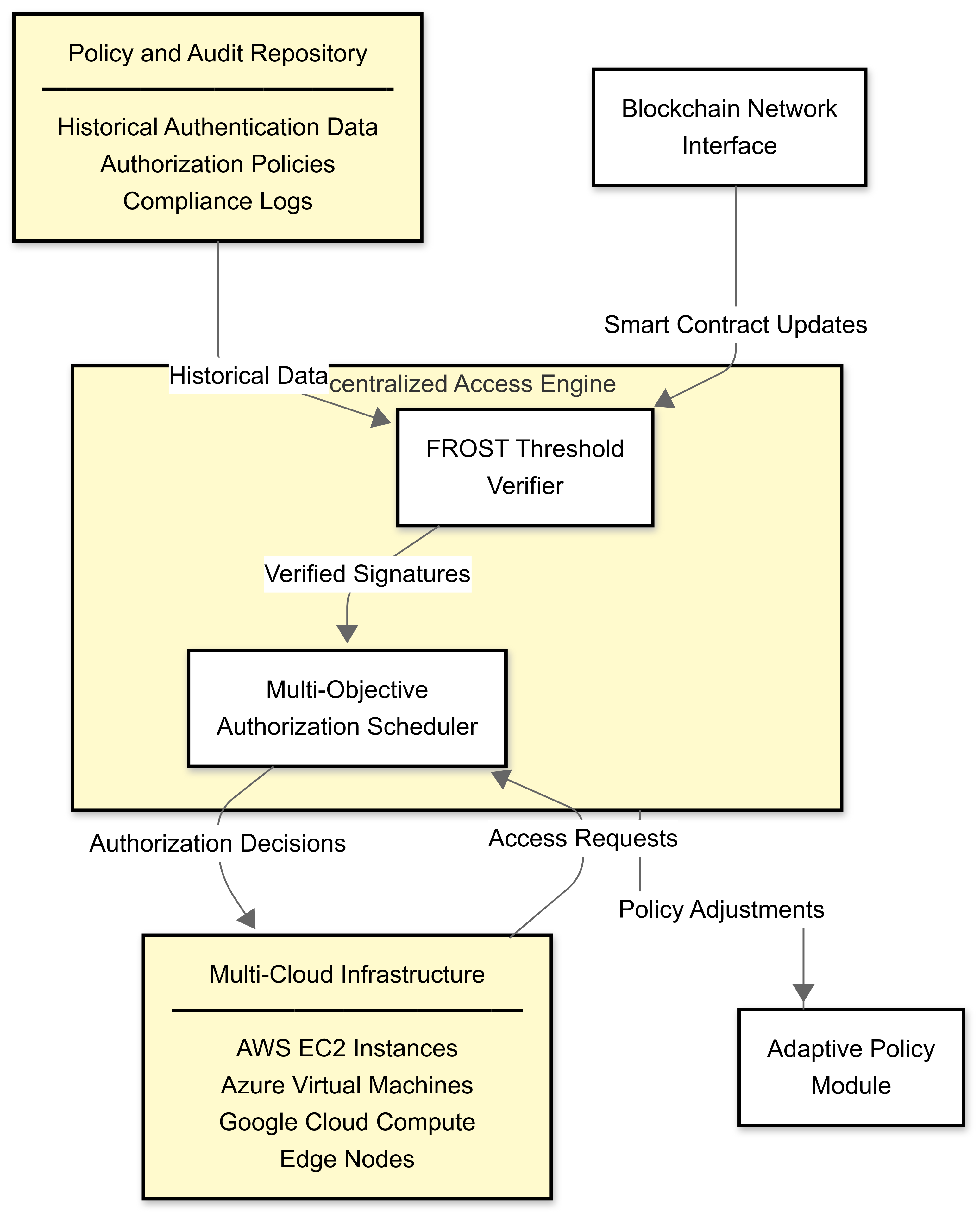
## Research Niche

The discussion of existing literature results in the identification of gaps that are targeted by this research. First, despite their superior characteristics, the FROST threshold signatures have never been linked to gas-optimized smart contracts in integrated form for real-time access control. Current blockchain IAM systems make use of multi-signature schemes of a traditional nature with O(n) on-chain storage and linear gas costs, resulting in limited scalability. Second, multi-cloud integration schemes still remain underdeveloped. Most research focuses on single-cloud deployments or theoretical federation models without production-ready implementations. Third, extensive performance comparisons on decentralized systems and traditional IAM systems under realistic workload conditions are negatively conspicuous in the existing literature.

The background paper by (Punia et al., 2024) gives a comprehensive overview of the previous solutions and sets basic metrics to be measured. Their metrics can be used to give tangible goals that are to be surpassed by our proposed system utilizing FROST integration and optimization strategies. Our innovation is a multifaceted one that consists of a series of innovations that are presented in a unified system architecture compared to currently available literature. The combination of FROST threshold signatures and gas optimized smart contracts has solved the security problem and the economics problem in one stroke. The creation of integration-ready API gateways that can be used on AWS and Azure enables the development of feasible implementation channels in enterprises. Most notably, our extended evaluation model provides new guidelines by which to benchmark blockchain-based IAM systems, as it does not only focus on usual performance parameters but also on the detection rates of security incidents, interconnection between clouds, and the ability to comply with regulations .

# Research Method & Specification

## Research Method

The proposed approach applies a hierarchical configuration to decentralized cloud resource access control using FROST threshold cryptography alongside gas-optimized smart contracts. The system is built on five interconnected modules that are arranged in a feedback-driven manner which allows the adaptive optimization of authority decisions based on real-time measurements and historical access patterns. The Policy and Audit Repository is the immutable store of access control features, authorization histories, and compliance audit trails. Furthermore, this database presents historical authentication events such as successful and failed access attempts, policy violations, and threshold signature events. The authorization policies are represented as Merkle trees, the structure enabling to generate proofs of specific permissions in a time-efficient way without the revelation of the whole policy structure. Compliance logs are the maintained records of all authorization decisions which are based on cryptographic signing, proving that regulatory requirements for auditability and non-repudiation are considered.

**Figure 1: Proposed Research Methodology**

The Decentralized Access Control Engine is composed of two integrated components which are responsible for the core authorization logic. The FROST Threshold Verifier checks multi-party signatures through RFC 9591 defined protocol, realizing t-of-n threshold schemes for a configurable amount of signature generators required from n total participants. The Multi-Objective Authorization Scheduler finds optimized access decisions for competing objectives which include the following: a target of minimum authentication latency less than 200ms, to reduce gas consumption lower than 30,000 gas units, and ensure the maximum count of f = ⌊(n-1)/3⌋ faulty nodes relative to n by maintaining the system's safety. The Multi-Cloud Infrastructure component stands for the distributed cloud resources primarily responsible for access control, which are AWS EC2 instances in us-east-1 and eu-west-1 regions. Access requests arise from these resources and are forwarded via the authorization engine for threshold signature validation.

The Blockchain Network Interface is the connection with Ethereum mainnet and Layer 2 solutions such as Arbitrum and Optimism. This module expresses the authorization decisions in the form of smart contract transactions, taking action on the gas optimization strategies carried out in the recent wave of network congestion that banked on dynamic fee adjustment management, while also overseeing the incurred limits due to congestion. Additionally, interface keeps pools to multiple RPC endpoints to secure resilient response to any single node failure encounter. The Adaptive Policy Module is built with continual optimization through reinforcement learning algorithms. As benchmark metrics, the success rates of authorization, the average response times, the gas consumption patterns, and the frequencies of security incidents are taken into consideration during feedback to policy optimizer. The feedback loop works perfectly to adjust the threshold parameters dynamically, in accordance with the variations that occur in the threat landscape and workload characteristics while holding the security guarantees intact.

## Implementation Steps and Activities

The planned implementation is a sequential process made of five phases:

* Phase 1 is the development stage of the threshold signature , coded in Solidity, and optimized for gas consumption assembly-level code where it's reasonable, thus saving gas . The stage also includes the development of distributed key generation protocols by supporting both trusted dealer and DKG approaches. A keychain refresh mechanism is created to allow dynamic participant management of the key without interruption of service.
* The access control primary smart contracts in the architecture are designed and implemented using the newly proxy pattern for extensibility purposes in Phase 2. The storage structures are developed using gas-optimized packed structs and hash tree commitments for the management of policies. The introduction of a circuit breaker option to react to emergencies and the gradual rollout competence are mechanisms included in the design.
* The API Gateway will build AWS and Azure RESTful API integration, event OAuth 2.0 flows with Ethereum-backed authentication in Phase 3. The WebSocket interfaces will provide the means for real-time authorization updates and event streaming. The SDK will be accessible in a variety of programming languages thus making it easier to build applications.
* The HotStuff consensus protocol for Byzantine fault tolerance is considered for the integration of modifications for access control use cases in Phase 4. The ROAST wrapper is there to ensure the signature completion under conditions of adversarial during execution. The maintenance of system availability Is done by the development of network partition detection and automatic recovery mechanisms.
* The Optimistic Rollups are developed in the final phase for first Layer 2 scaling solution that will be deployed to increase operation frequency. Data caching will be brought into effect at the API gateway layer to minimize blockchain interactions. The smart contract code will be optimized through the profiling period and through assembly-level improvements where justifiable gas savings are presented.

## Research Resources

The evaluation process is based on actual datasets from cloud enterprise deployment setups to ensure real practical relevance. The primary dataset consists of the anonymized AWS CloudTrail[[1]](#footnote-2) logs of a Fortune 500 company containing 10 million access requests through 1,000 IAM roles and 50,000 resources for 90 days. The dataset mirrors those of enterprises that typically exhibit a mix of seasons which include jobs scheduled periodically, traffic which spikes suddenly, and cross-account permission which seem complex. A secondary dataset from Azure Activity Logs exhibits the events 5 million authorization through 500 applications thus permitting multi-cloud scenario tests.

Cloud platforms for deployment include AWS with services such as the ECS for container orchestration, Lambda for serverless components, and CloudFormation for infrastructure as code. In azure, one employs AKS to orchestrate Kubernetes, functions to process events, and ARM Templates to automate the deployment. The multi-cloud architecture involves utilizing Terraform to have a unified management of the infrastructure provided by multiple providers. A Layer 2 architecture that includes a private Ethereum network running 21 validator nodes that are spread across three geographic regions and Arbitrum One.

## Evaluation

The comparison is done between our proposed system, two baselines, traditional centralized IAM (AWS IAM and Azure AD), and state-of-the-art blockchain-based system that is centered on (Punia et al., 2024). The evaluation metrics include transactions per second (TPS) at different loads up to 10,000 concurrent requests, end-to-end latency (or time) of an authorization request measured in start request to access token generation, and gas costs of an operation in both USD and gas in gas units. Throughput has been investigated in terms of sustained load and burst traffic, resistance, and performance degradation to Byzantine attacks. Security analysis is carried out in terms of incident detection rates through an exercise of 50 attempted attack occasions, such as key compromise, policy alteration as well as, consensus destruction. The MTTD and MTTR are quantitative security measures. Byzantine fault tolerance testing checks what the system does with a different amount of malicious nodes, checking availability, safety violations, and convalescence period. The analysis will be performed about sensitivity over Ethereum gas price changes and its effects on operational costs. Scalability testing tests performance as the numbers of participants in a threshold signature scheme, combined edges of control policies, and the number of concurrent users addresses set the job to test.

## Ethical Considerations of the Research

The research is conducted in agreement with the rigorous ethical guidelines that guarantee the responsibility of the development and implementation of decentralized access control systems. Privacy protection is of the utmost importance, and all the datasets used in the evaluation will be anonymized with the help of differential privacy to exclude the possibility of re-identification of individuals or organizations. The implementation contains privacy-aspects like zero-knowledge proofs of sensitive authorization decisions so that relationships between access patterns do not reveal confidential compromising information about users or resources. Security vulnerability disclosure is based on the responsible disclosure, thus any security vulnerabilities identified on existing systems would be disclosed to vendors prior to full public disclosure.

The effect on the environment is a factor that recognizes the energy use of blockchain technology. The study gives priority to the Ethereum Proof of Stake (PoS) that consumes 99.95 percent less energy than Proof-of-Work systems. The environmental impact is also reduced through methods of batching transactions with layer level 2 scaling solutions. The assessment will involve carbon footprint, and it will analyze how our system compares with the old data center-based implementation of IAM.

## A diagram of a projectProject Plan

Figure 2 Project Timeline Chart

# Conclusion

The work provides a strategy of decentralized cloud resource access control by introducing FROST threshold cryptography combined with a gas-optimal multi-signature smart contract. The suggested architecture supports the most significant weaknesses of centralized IAM systems, such as absence of single points of failure, transparent audit trail, and Byzantine fault-tolerant authorization across multi-clouds. By systematizing the optimization of smart contract operations and integration with Layer 2 scalability solutions, the network is able to offer latencies of sub-second authorization latency to the enterprise category intended to lower operational costs as compared to conventions. The research has introduced a basis of further developments in decentralized identity management area where it is proved that blockchain-based access control may suit the security and performance demands of contemporary cloud infrastructure.

# References

Cimatti, A., De Sclavis, F., Galano, G., Giammusso, S., Iezzi, M., Muci, A., Nardelli, M. and Pedicini, M. (2025). Dynamic-FROST: Schnorr threshold signatures with a flexible committee. *Journal of Mathematical Cryptology*, 19(1). doi:<https://doi.org/10.1515/jmc-2024-0045>.

Connolly, D., Komlo, C., Goldberg, I. and Wood, C.A., 2024. *The Flexible Round-Optimized Schnorr Threshold (FROST) Protocol for Two-Round Schnorr Signatures*. RFC 9591. June 2024. doi: 10.17487/RFC9591. url: https://www. rfc-editor. org/info/rfc9591.

He, M., Xia, S., Qin, B., Yoshida, N., Yu, T., Song, L. and Zhang, Y. (2024). *How to Save My Gas Fees: Understanding and Detecting Real-world Gas Issues in Solidity Programs*. [online] arXiv.org. Available at: <https://arxiv.org/abs/2403.02661> [Accessed 18 Sep. 2024].

Hu, V.C. (2022). Blockchain for Access Control Systems. [online] doi:<https://doi.org/10.6028/nist.ir.8403>.

Khanzadeh, S. and Alalfi, M.H. (2024). SolOSphere: A Framework for Gas Optimization in Solidity Smart Contracts. *2024 IEEE International Conference on Software Analysis, Evolution and Reengineering - Companion (SANER-C)*, [online] pp.35–45. doi:<https://doi.org/10.1109/saner-c62648.2024.00010>.

Kim, H. and Kim, D. (2024). Optimal Gas Fee Minimization in DeFi: Enhancing Efficiency and Security on the Ethereum Blockchain. *IEEE Access*, [online] 12, pp.173810–173823. doi:<https://doi.org/10.1109/access.2024.3495714>.

Komlo, C. and Goldberg, I. (2021). FROST: Flexible Round-Optimized Schnorr Threshold Signatures. *Lecture notes in computer science*, pp.34–65. doi:<https://doi.org/10.1007/978-3-030-81652-0_2>.

Li, J., Zhao, Z., Su, Z. and Meng, W. (2023a). Gas-expensive patterns detection to optimize smart contracts. *Applied Soft Computing*, [online] 145, p.110542. doi:<https://doi.org/10.1016/j.asoc.2023.110542>.

Li, W., Meese, C., Nejad, M. and Guo, H. (2023b). ZK-BFT: A Zero-knowledge and Byzantine Fault Tolerant Consensus for Permissioned Blockchain Networks. *Proceedings of the 2023 6th International Conference on Blockchain Technology and Applications*, pp.70–77. doi:<https://doi.org/10.1145/3651655.3651663>.

Moyo, L. and Jaco du Toit (2024). The Use of Blockchain for Identity and Access Management (IAM) in Multi-cloud. *Lecture notes in networks and systems*, pp.149–159. doi:<https://doi.org/10.1007/978-981-97-3302-6_13>.

Muddychetty, Nithya Sree (2024). *A Comparative Analysis of SecurityServices Using Identity and AccessManagement (IAM)*. [online] DIVA. Available at: <https://www.diva-portal.org/smash/record.jsf?pid=diva2%3A1842261&dswid=3633> [Accessed 27 Jul. 2025].

Nelaturu, K., Beillahi, S.M., Long, F. and Veneris, A., 2021, September. Smart contracts refinement for gas optimization. In *2021 3rd conference on blockchain research & applications for innovative networks and services (BRAINS)* (pp. 229-236). IEEE.

Punia, A., Gulia, P., Gill, N.S., Ibeke, E., Iwendi, C. and Shukla, P.K. (2024). A systematic review on blockchain-based access control systems in cloud environment. *Journal of Cloud Computing*, [online] 13(1). doi:<https://doi.org/10.1186/s13677-024-00697-7>.

Ruffing, T., Ronge, V., Jin, E., Schneider-Bensch, J. and Schröder, D. (2022). ROAST: Robust Asynchronous Schnorr Threshold Signatures. *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*. doi:<https://doi.org/10.1145/3548606.3560583>.

1. https://www.kaggle.com/datasets/nobukim/aws-cloudtrails-dataset-from-flaws-cloud [↑](#footnote-ref-2)