# Practical and Secure NFT Access Control for Low-Cost IoT Devices via a Delegated Reputation Gateway

Pedro F. F. Abreu[1], Maria R. F. M. Ferreira[1], Luis H. O. Mendes[1],
Geraldo A. Sarmento Neto[1], Thiago A. R. da Silva[1,2], Anderson L. Sanches[3],
Ricardo A. L. Rabelo[1] and José V. dos Reis Junior[1]
[1]*Federal University of Piauí (UFPI), Teresina - Piauí*, [2]*Federal Institute of Maranhão (IFMA), Barra do Corda - Maranhão*
[3]*Federal University of ABC (UFABC), Santo André - São Paulo*
{pedroffda, maria.ferreira, luishenriqueom, geraldosarmento, thiago.allisson, ricardoalr, valdemirreis}@ufpi.edu.br,
anderson.sanches@ufabc.edu.br

***Abstract*—The proliferation of Internet of Things (IoT) devices necessitates secure, scalable, and cost-effective access control mechanisms. While blockchain and Non-Fungible Tokens (NFTs) offer a decentralized paradigm for managing permissions, they remain vulnerable to off-chain resource exhaustion attacks and present practical implementation challenges for low-cost devices. This paper proposes a novel hybrid architecture that enhances NFT-based access control with an off-chain gateway acting as both a Smart Reputation System (SRS) and a delegated signer. This hybrid model combines fast, off-chain pre-validation with authoritative on-chain verification. The SRS serves as a security firewall, mitigating high-frequency invalid requests by dynamically managing the reputation of each device and imposing temporary bans on malicious actors. By delegating cryptographic signing to the gateway, low-cost IoT devices are absolved of managing private keys, significantly reducing their complexity and cost. An experimental evaluation of the implemented system was conducted to assess its resilience against Denial-of-Service attacks. The findings indicate that the system successfully neutralizes threats in under 3 seconds. During this process, a stable end-to-end latency of approximately 626 ms is maintained for legitimate users, with the gateway's reputation logic introducing a negligible performance overhead of less than 1%. This hybrid approach proves to be a practical and effective solution for deploying secure and resilient access control in real-world IoT environments.**

***Index Terms*—Access Control, Blockchain, IoT, NFT, Reputation System**

## I. Introduction

The Internet of Things (IoT) ecosystem is expanding at an unprecedented rate, connecting billions of devices across critical sectors [1], [2]. This hyper-connectivity introduces significant security challenges, particularly in access control, where traditional centralized models often fail to provide the necessary scalability, auditability, and resilience [3].

Blockchain technology [4], particularly through Non-Fungible Tokens (NFTs), has emerged as a promising solution for decentralized access control [5]. By representing access rights as unique tokens on an immutable ledger, NFTs provide a trustless foundation for managing permissions. However, two primary challenges hinder their adoption in IoT: (1) high computational overhead of on-chain operations makes systems vulnerable to off-chain resource exhaustion attacks (e.g., Denial-of-Service), and (2) requiring each low-cost IoT device to securely manage a private key is often impractical from a hardware and cost perspective.

To address these challenges, this paper proposes a novel hybrid architecture that leverages an off-chain gateway integrating a Smart Reputation System with a delegated signing mechanism. The hybrid approach employs an off-chain gateway for high-frequency, stateful reputation checks, while relying on the on-chain NFT ownership as the low-frequency, authoritative source of truth. The system utilizes standard technologies: NFTs following the ERC-721 standard [6] provide the access credentials, and the lightweight Message Queuing Telemetry Transport (MQTT) protocol [7] handles communication for constrained devices. Acting as a security-aware intermediary, this gateway provides a critical first line of defense. The main contributions of this work are:

- A hybrid on-chain/off-chain model that protects against resource exhaustion attacks by implementing an off-chain reputation system to pre-validate requests.
- A delegated signer architecture that simplifies IoT device requirements by centralizing private key management.
- An empirical evaluation of the system's performance and resilience, providing quantitative data on its ability to neutralize attacks while maintaining low latency for legitimate users.

## II. Related Work

The challenge of securing IoT access control has been addressed through various paradigms. Traditional models like Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC), when adapted for IoT [8], introduce a single point of failure at the central authorization server. To overcome this, researchers proposed blockchain-based solutions, initially storing access control policies directly on-chain [9]. While enhancing security, this approach often incurs high transactional costs and latency, and fails to protect

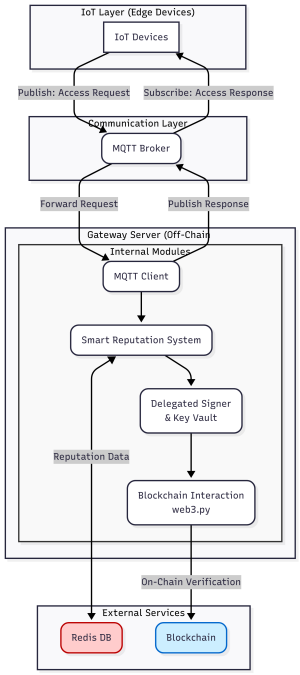


Fig. 1. High-level architecture of the hybrid access control system.

against off-chain resource exhaustion attacks, where a device is overwhelmed before any on-chain transaction occurs.

More recently, the use of NFTs as transferrable, fine-grained "keys" for access control has gained traction [10]–[13]. However, existing literature largely overlooks two critical practical challenges. First, it often fails to mitigate off-chain Denial-of-Service vulnerabilities at the system's entry points [14]. Second, these models frequently presume that low-cost IoT devices possess the capability to securely store private keys and perform cryptographic signing operations, a significant barrier to large-scale deployment. This work directly addresses these gaps by positioning an off-chain SRS as a first line of defense and incorporating a delegated signer model, bridging the gap between theoretical NFT security and the practical requirements of real-world IoT systems.

## III. Proposed System Architecture

The proposed system provides a secure and resilient access control layer for IoT environments by decoupling high-frequency, stateful reputation checks from low-frequency, authoritative on-chain verification. This hybrid architecture, illustrated in Fig. 1, is composed of four main layers: the IoT Device Layer, a Communication Layer, the Gateway Server, and the External Services Layer:

- IoT Device Layer: Consists of resource-constrained edge devices, e.g., ESP8266, responsible only for sending access requests and receiving responses over MQTT.
- Communication Layer: A standard MQTT broker serves as the communication backbone.
- Gateway Server Layer: The core of the solution, it hosts the SRS and the Delegated Signer.

**Algorithm 1:** Gateway Access Request and Reputation Logic

**Input:** Device ID: *device_id*, Request payload: *payload*
**Output:** *AccessGranted* or *AccessDenied*

```
/* 1. Firewall Check (Off-Chain)                          */
if database.exists("ban:" + device_id) then
    return AccessDenied ;        // Block banned devices
/* 2. On-Chain Verification                               */
privateKey ← keyVault.get(device_id)
if privateKey is null then
    hasAccess ← false ;          // Device is unregistered
else
    walletAddress ← deriveAddress(privateKey)
    token_id ← payload.get('token_id')
    hasAccess ← SmartContract.hasAccess(token_id, walletAddress)
/* 3. Reputation Update (Off-Chain)                       */
repKey ← "reputation:" + device_id
data ← database.get(repKey) or {score : 100, streak : 0} if
  hasAccess then
    data.score ← data.score + SCORE_INCREMENT
    data.streak ← 0
    database.set(repKey, data)
    return AccessGranted
else
    data.score ← data.score − SCORE_DECREMENT
    data.streak ← data.streak + 1
    database.set(repKey, data)
    /* Check for ban condition after update           */
    if data.score < BAN_THRESHOLD or
      data.streak ≥ MAX_STREAK then
        database.set("ban : " + device_id, "banned", EX =
          BAN_DURATION)
    return AccessDenied
```

- External Services Layer: Includes a high-speed Redis database for reputation data and the public blockchain (e.g., Polygon) which serves as the ultimate source of truth.

The interaction begins when a device publishes an access request. The request is routed through the MQTT broker to the Gateway Server, where the full verification and reputation logic is executed.

### A. Smart Reputation System (SRS) Gateway

The core of the architecture is the gateway's SRS. This off-chain component acts as a stateful firewall, maintaining a reputation score for each device ID in Redis. The gateway's logic is detailed in Algorithm 1. For every incoming request, it first checks if a device is banned. If not, it proceeds to the on-chain verification. Based on the on-chain result, the gateway updates the device's reputation, allowing it to dynamically identify and isolate malicious actors.

### B. Delegated Signer and Key Vault

To alleviate hardware constraints, the gateway functions as a delegated signer. It maintains a secure "key vault," mapping each device ID to its blockchain private key. When a request is received, the gateway signs the on-chain query on the device's behalf. This abstracts away cryptographic complexity from the end device.While this model is optimized for constrained

devices, the architecture allows for more capable devices to manage their own keys and interact directly with the blockchain, bypassing the delegated signing feature.

## IV. Experimental Setup

### A. Environment, Threat Model, and Implementation

The experimental environment consisted of a Gateway Server (Avell B.ON, 12th Gen Intel® Core™i7-1255U, 16.0 GiB RAM) hosting all backend services, and a low-cost ESP8266 IoT Device. The software stack included Python/FastAPI [1] for the backend logic, Redis [2] for in-memory reputation data storage, and a Mosquitto MQTT broker [3], with all services containerized via Docker [4] for consistency. The IoT device firmware was developed in the Arduino IDE.

The threat model considered in this work focuses on off-chain resource exhaustion attacks, Denial-of-Service, a practical vulnerability for IoT gateways where malicious actors flood the system with invalid requests to consume computational resources and prevent service to legitimate users, all without incurring on-chain costs. This experiment simulates a single-source DoS attack, representing a common scenario of a compromised device or targeted script.

For blockchain interactions, the `IoTAccessNFT` smart contract was deployed on the Polygon network via an Alchemy RPC node. This ERC-721 compliant contract implements a core function, `hasAccess(tokenId, userAddress)`, which returns `true` only if the address is the owner of the NFT, serving as the definitive authority for permission verification.

### B. Test Scenarios and Parameters

To evaluate the system, two scenarios were designed, each running for a total of 5 minutes to gather stable measurements. The tests involved a Legitimate User ESP8266 and an Attacker, a Python script.

1) **Baseline Performance Scenario:** This test measured performance under normal conditions. The Legitimate User sent valid requests at a steady rate of 1 request per second (1 Hz) to establish a baseline for end-to-end latency ($T_{e2e}$).
2) **Resilience Scenario (DoS Attack):** This test evaluated the SRS's effectiveness. While the Legitimate User maintained its 1 Hz request rate, the Attacker simulated a DoS attack by sending invalid requests, using a valid device ID but an unauthorized `token_id`, at a rate of 10 requests per second (10 Hz). The SRS was configured with a `MAX_STREAK` of 3 consecutive failures to trigger a ban and a `BAN_DURATION` of 300 seconds.

## V. Results and Discussion

The experimental results validate the efficacy and efficiency of the proposed hybrid architecture.

[1]https://fastapi.tiangolo.com/
[2]https://redis.io/
[3]https://mosquitto.org/
[4]https://www.docker.com/

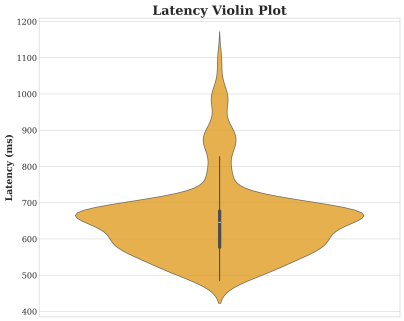


Fig. 2. Density plot of end-to-end latency for legitimate user requests under baseline conditions (1 req/s).

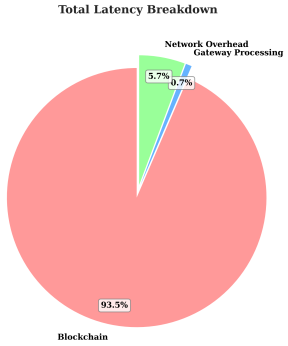


Fig. 3. Breakdown of the average total latency, highlighting the dominance of the on-chain verification step.

### A. Baseline Performance Analysis

Under normal operating conditions, the system demonstrated a stable and largely predictable performance profile. The end-to-end latency for legitimate user requests is visualized in the violin plot in Fig. 2. The plot's shape reveals a high concentration of data points within the 600-700 ms range, indicating a consistent response time. The internal box plot specifies a median latency of approximately 640 ms. Despite some outliers, the overall average latency remained stable at 626 ms.

A decomposition of this average latency, Fig. 3 reveals that on-chain verification is the primary bottleneck, accounting for 93.5% of the total processing time. In contrast, the gateway logic, including reputation checks, contributed a negligible 0.7%. This confirms the SRS acts as an efficient firewall without introducing significant overhead.

### B. Resilience Against High-Frequency Attacks

To evaluate resilience against hostile traffic, a DoS attack was simulated. The system's response is illustrated in Fig. 4. Faced with the 10 Hz attack, the gateway correctly identified the first three invalid requests. Upon the third consecutive failure, matching the configured `MAX_STREAK` threshold, it activated a temporary ban. The attacker was blocked in approximately 2.7 seconds. Throughout the attack, latency for the legitimate user remained stable, demonstrating the system's ability to isolate threats without impacting valid operations.

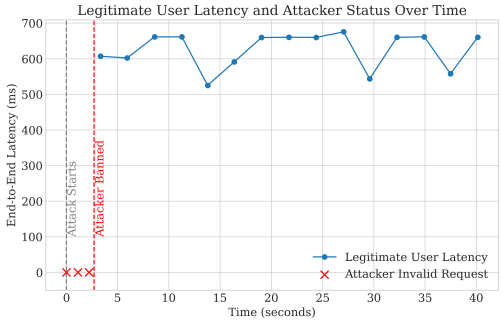


Fig. 4. End-to-end latency for a legitimate user during a simulated DoS attack. The SRS detects and bans the attacker (red crosses and dashed line) in under 3 seconds, while legitimate user latency remains stable.

Structured JSON logs generated by the gateway provided clear, auditable evidence. A successful request log detailed the on-chain verification time, while the log immediately following the ban showed an *ACCESS_DENIED_BANNED* outcome, where the on-chain verification step was skipped entirely, 0 *ms* processing time. This confirms the gateway acts as an effective off-chain firewall, protecting the blockchain from unnecessary load.

### C. Economic Viability and Cost Analysis

Beyond technical performance, the economic viability of the proposed off-chain gateway architecture was considered. While a previous analysis confirmed that on-chain transaction costs for administrative tasks like minting are negligible on Layer-2 networks like Polygon [13], this work focuses on the operational costs of the off-chain infrastructure. The operational costs are minimal: a self-hosted model, co-locating the gateway, MQTT broker, and Redis database on a single low-cost virtual private server (e.g., a DigitalOcean Droplet), is highly cost-effective at approximately $5-10 per month. For higher reliability, using managed cloud services (e.g., AWS EC2 for compute and ElastiCache for Redis) remains modest, with total costs estimated at $20-35 per month. Crucially, the ongoing cost for blockchain interaction is minimal, as RPC providers like Alchemy offer generous free tiers sufficient for the read-only queries required. This cost analysis confirms that the proposed hybrid architecture is not only technically resilient but also economically practical for real-world IoT applications.

## VI. Conclusion and Future Work

This paper addressed the critical challenge of implementing secure yet practical NFT-based access control for resource-constrained IoT environments. A novel hybrid architecture was presented, featuring an off-chain gateway that integrates a SRS with a delegated signing model. This design enhances security by mitigating resource exhaustion attacks and improves practicality by simplifying implementation on low-cost devices.

The empirical validation of this hybrid model's efficiency is the central contribution. Experimental results reveal that the resource-intensive on-chain verification constitutes 93.5% of request latency, while the entire off-chain gateway logic accounts for a negligible 0.7%. This efficiency enables the gateway to neutralize high-frequency attacks in under 3 seconds while maintaining stable performance for legitimate users. Complemented by a cost analysis showing that the required off-chain infrastructure can operate for as little as $5-10 per month, the proposed system is demonstrated to be not only secure and scalable but also economically viable for real-world IoT applications.

Future research could extend this work in several key directions. These include: (1) integrating Decentralized Identifiers to enhance user privacy; (2) developing adaptive reputation algorithms, potentially using machine learning, to detect more complex attack patterns; and (3) conducting a long-term, large-scale deployment to further validate the system's scalability and operational costs.

## References

[1] I. P. Okokpujie and L. K. Tartibu, "Study of the economic viability of internet of things (iots) in additive and advanced manufacturing: A comprehensive review," *Progress in Additive Manufacturing*, vol. 10, no. 5, pp. 3175–3194, 2025.

[2] M. A. Guimarães and R. J. D. A. Macêdo, "Energy-efficient ehealth monitoring with lpwan," in *2024 XIV Brazilian Symposium on Computing Systems Engineering (SBESC)*. IEEE, 2024, pp. 1–6.

[3] N. Farhadighalati, L. A. Estrada-Jimenez, S. Nikghadam-Hojjati, and J. Barata, "A systematic review of access control models: Background, existing research, and challenges," *IEEE Access*, 2025.

[4] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," May 2009. [Online]. Available: http://www.bitcoin.org/bitcoin.pdf

[5] L. Ante and I. Fiedler, "The new digital economy: How decentralized finance (defi) and non-fungible tokens (nfts) are transforming value creation, ownership models, and economic systems," p. 100094, 2025.

[6] S. Casale-Brunet, P. Ribeca, P. Doyle, and M. Mattavelli, "Networks of ethereum non-fungible tokens: A graph-based analysis of the erc-721 ecosystem," in *2021 IEEE International Conference on Blockchain (Blockchain)*. IEEE, 2021, pp. 188–195.

[7] O. Standard, "Mqtt version 3.1. 1," *URL http://docs. oasis-open. org/mqtt/mqtt/v3*, vol. 1, p. 29, 2014.

[8] M. S. Ahsan and A.-S. K. Pathan, "A comprehensive survey on the requirements, applications, and future challenges for access control models in iot: The state of the art," *IoT*, vol. 6, no. 1, 2025. [Online]. Available: https://www.mdpi.com/2624-831X/6/1/9

[9] P. Nemala, B. Chen, and H. Cui, "A privacy preserving attribute-based access control model for the tokenization of mineral resources via blockchain," *Applied Sciences*, vol. 15, no. 15, p. 8290, 2025.

[10] S. A. Gebreab, H. R. Hasan, K. Salah, and R. Jayaraman, "Nft-based traceability and ownership management of medical devices," *IEEE Access*, vol. 10, pp. 126 394–126 411, 2022.

[11] W. Wang, H. Huang, Z. Yin, T. R. Gadekallu, M. Alazab, and C. Su, "Smart contract token-based privacy-preserving access control system for industrial internet of things," *Digital Communications and Networks*, vol. 9, no. 2, pp. 337–346, 2023.

[12] A. Musamih, K. Salah, R. Jayaraman, S. Ellahham, M. Omar, and I. Yaqoob, "Blockchain and nft-based solution for genomic data management, sharing, and monetization," *IEEE Access*, 2025.

[13] P. F. F. Abreu, M. R. F. M. Ferreira, G. A. Sarmento Neto, T. A. R. da Silva, G. D. Gonçalves, R. A. L. Rabelo, and J. V. dos Reis Junior, "Decentralized IoT permission management using NFTs: Implementation and evaluation on low-cost blockchains," in *Proceedings of the 12th International Conference on Future Internet of Things and Cloud (FiCloud)*, 2025, in press.

[14] M. R. Hasan, A. Alazab, S. B. Joy, M. N. Uddin, M. A. Uddin, A. Khraisat, I. Gondal, W. F. Urmi, and M. A. Talukder, "Smart contract-based access control framework for internet of things devices," *Computers*, vol. 12, no. 11, p. 240, 2023.