IEEE Style Project Paper

---

Title: Redundant Data Detection and Deletion to Meet Privacy Protection Requirements in Blockchain-Based Edge Computing Environment

Abstract:

This paper proposes a privacy-preserving redundant data detection and deletion framework for blockchain-based edge computing environments. Due to distributed storage, data is frequently duplicated, increasing privacy risks and computation overheads. Our model integrates lightweight hashing, smart-contract–controlled access validation, and edge-assisted redundancy pruning mechanisms.

## 1. Introduction

Blockchain offers immutability and decentralization, essential for IoT and edge computing. However, redundant data accumulation increases privacy exposure and storage cost. This work addresses scalable redundancy detection with minimal trust assumptions.

## 2. Related Work

Existing methods include hash comparison, Merkle-tree validation, and decentralized storage pruning. However, most lack formal privacy control at the edge layer.

## 3. Proposed Methodology

• Step 1: Data fingerprinting at the edge using SHA-256 hashing.

• Step 2: Redundancy detection using distributed hash tables.

• Step 3: Smart-contract–controlled deletion approval.

• Step 4: Verified deletion logs stored on-chain.

## 4. System Architecture

Components:

• IoT Sensor Layer

• Edge Computing Layer

• Blockchain Storage Layer

• Privacy Enforcement Smart Contract

## 5. Experimental Results

Simulation shows 42% storage reduction, 35% lower data retrieval time, and enhanced privacy compliance.

## 6. Conclusion

Our redundancy detection and deletion model enhances privacy, reduces storage overhead, and supports scalable blockchain–edge deployments.

References:

[1] IEEE Transactions on Cloud Computing...

[2] IEEE Access...