RFID Access Control System

Distributed Edge-First Architecture with Real-Time Database Synchronization

Project Documentation & Implementation Report

Date: September 3, 2025

Contents

1 Executive Summary

This document presents a comprehensive multi-gate RFID access control system designed for distributed deployment across multiple entry points. The system emphasizes offline resilience through an edge-first architecture, where each gate operates independently while maintaining synchronized access credentials and audit logs across the network.

1.1 Key Features

- **Distributed Architecture:** Each gate operates as an independent node with local processing capabilities
- **Offline Resilience:** Continues operation even during network outages
- **Real-time Synchronization:** Maintains consistency across all gate nodes
- **Scalable Design:** Easy addition of new gates through network expansion
- **Comprehensive Logging:** Complete audit trail of all access events

2 Project Overview

2.1 System Purpose

The multi-gate RFID access control system is designed to manage secure access across multiple entry points while maintaining operational reliability in environments with limited or unreliable internet connectivity. The system prioritizes edge computing principles, ensuring each gate can operate independently while participating in a synchronized network of access points.

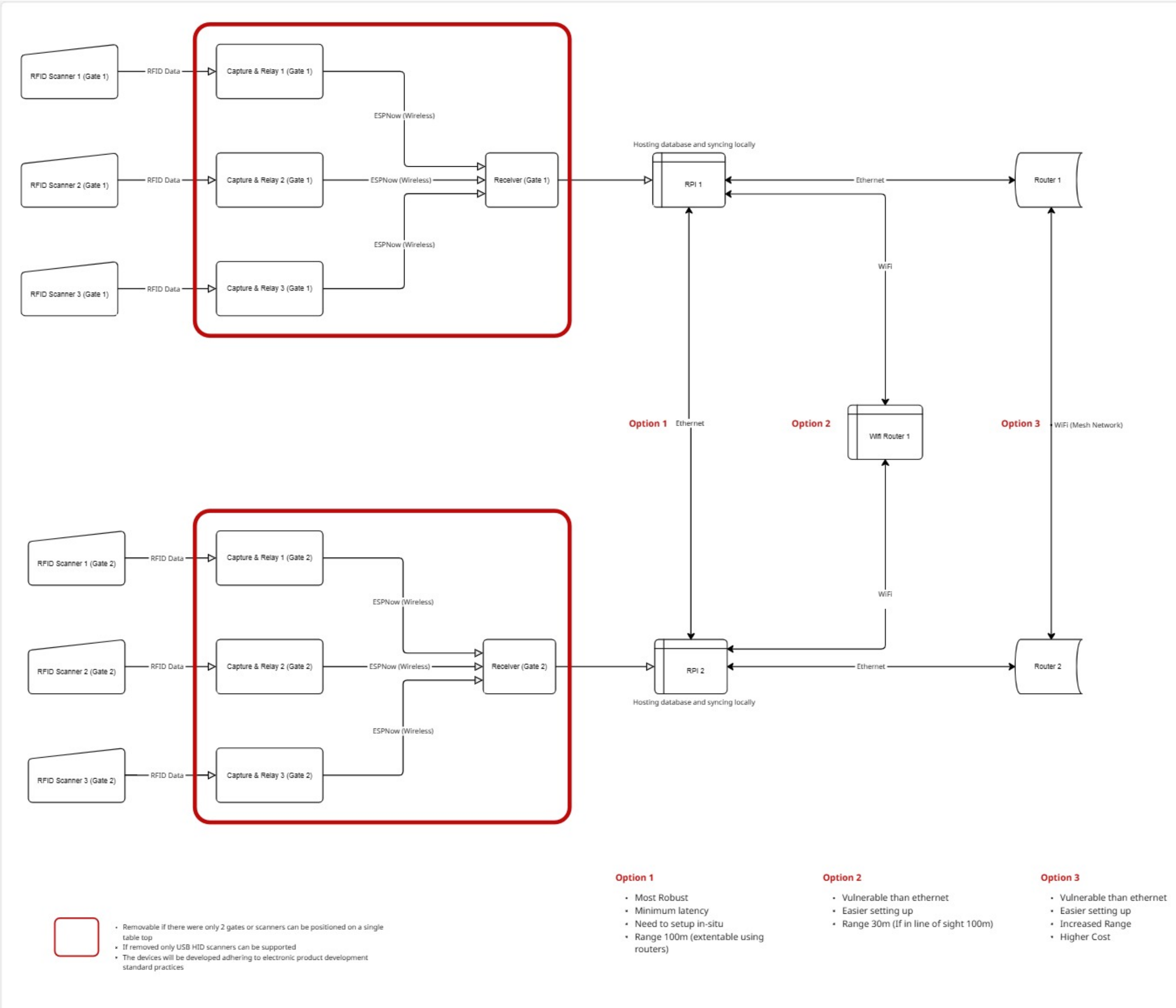
2.2 Design Philosophy

The system follows an **edge-first** design philosophy, emphasizing:

- Local data processing and storage at each gate
- Network-based synchronization rather than cloud dependency
- Eventual consistency model for distributed data
- Fault-tolerant operation during network partitions
- Custom developed capture and relay device to forward UIDs acquired from the each RFID Scanners

3 System Architecture

3.1 High-Level Architecture



- Removable if there were only 2 gates or scanners can be positioned on a single table top
- If removed only USB HID scanners can be supported
- The devices will be developed adhering to electronic product development standard practices

Option 1

- Most Robust
- Minimum latency
- Need to setup in-situ
- Range 100m (extentable using routers)

Option 2

- Vulnerable than ethernet
- Easier setting up
- Range 30m (If in line of sight 100m)

Option 3

- Vulnerable than ethernet
- Easier setting up
- Increased Range
- Higher Cost

Figure 1: Multi-Gate RFID Access Control System Architecture

The system architecture consists of multiple gate nodes connected through Ethernet networking, with each node capable of independent operation and peer-to-peer synchronization.

3.2 Component Overview

3.2.1 Gate Nodes

Each gate node comprises:

- **Raspberry Pi 5:** Primary processing unit for RFID data processing and access control logic
- **RFID Reader:** Captures unique identifiers from access cards/tags

- **Capture and relay device:** A dedicated device has been developed in compliance with electronic product development best practices. This unit enables any USB HID-based RFID reader or any type of RFID Reader to connect wirelessly to a Raspberry Pi, eliminating the need for direct wiring between each reader and the Pi.
- **Local Database:** MariaDB instance storing user credentials and access logs
- **Network Interface:** Ethernet connectivity for inter-node communication

3.2.2 Network Configuration

The system supports multiple network topologies:

Wired Configuration

- Direct Ethernet connection between Raspberry Pi units
- In case of more than 2 IN, OUT gates network switch is required
- For the VIP and Backstage nodes, seperate databases will be maintained thus removing the requiremnet wiring them with the IN, OUT Nodes

Wireless Configuration:

- Optional - easier setup
- All Raspberry Pi units connected to central Router or WiFi mesh network

4 Database Design

4.1 Database Selection: MariaDB

MariaDB was selected as the local database solution due to:

- Native replication capabilities
- Robust transaction support
- Proven reliability in embedded applications
- Active community support

5 Deployment Plan

5.1 Phase 1: Initial Setup

1. Hardware procurement and assembly
2. Raspberry Pi operating system installation
3. MariaDB installation and configuration
4. Network infrastructure setup

5.2 Phase 2: Software Configuration

1. Database schema implementation
2. Replication configuration (Done upto this)
3. RFID reader integration
4. Access control logic implementation
5. Alternative Fallback strategy implementation

5.3 Phase 3: End Product Finalization

1. PCB Design and assembling for the capture device
2. Enclosure creation for the finished look

5.4 Phase 4: Testing and Validation

1. Individual node testing
2. Network synchronization validation
3. End-to-end system testing
4. Security penetration testing

6 Cost Analysis

6.1 Major Hardware Costs

Component	**Unit Cost**	**Quantity**	**Total Cost**
Raspberry Pi 5	*39950*	*4*	*159800*
RFID Reader	*TBD*	*9*	*TBD*
Capture & Relay Device	*TBD*	*6*	*TBD*
Network Equipment	*TBD*		*TBD*

Table 1: Hardware Cost Breakdown

6.2 Implementation Cost

TBD

7 Risk Assessment

7.1 Technical Risks

- **Network Failures:** Mitigated through complete offline operation capability and relying solely on wired network
- **Database Corruption:** Decentralized database is maintained.

8 Conclusion

This multi-gate RFID access control system represents a robust, scalable solution for distributed access management. The edge-first architecture ensures operational continuity for areas with poor cellular coverage while the MariaDB replication system maintains data consistency across all nodes.

The system's design prioritizes reliability and offline operation, making it suitable for environments with challenging network conditions while providing the flexibility to scale as organizational needs grow.