Frontiers in Computing and Intelligent Systems
ISSN: 2832-6024 | Vol. 11, No. 1, 2025

Integration and Optimization of Cloud and Edge Computing in the Application Research of Cloud-based Management Platform for Airport Restricted Area Passes

Hao Tu [1, 2], Ping Zhang [1, 2], Tie Cao [1, 2]

[1] The Second Research Institute of CAAC, Chengdu Sichuan, 610041, China
[2] Civil Aviation Electronic Technology Co., Ltd, Chengdu Sichuan, 611430, China

Abstract: With the continuous expansion of global airport scales and the growing demand for enhanced security management, the management of airport restricted area passes faces multiple challenges in terms of efficiency, precision, and security. This paper focuses on the design and implementation of a cloud-based management platform for airport restricted area passes, exploring the application of integrated optimization techniques of cloud and edge computing within the platform. A cloud-edge collaborative architecture is proposed to enhance the efficiency of pass management, ensure data security, and optimize user experience. This platform provides a new solution and technical support for advancing the intelligent and standardized management of airport restricted area passes nationwide.

Keywords: Edge Computing; Cloud Platform; Airport Restricted Area Passes.

1. Introduction

The airport restricted area is the core region for ensuring the operational safety of airports, and its pass management plays a crucial role in maintaining airport security and order. However, traditional pass management models face challenges such as low efficiency in manual reviews, decentralized data storage, and difficulty in tracking management processes, making them inadequate to meet the increasingly complex operational demands of modern airports. With the global wave of informatization and digitalization, many airports have built their own restricted area pass management systems to improve pass management efficiency. However, these systems are often locally deployed, requiring significant investments, lacking flexibility, and resulting in data being scattered across different locations within the airport, making unified supervision difficult[1].

With the rapid development of technologies such as cloud computing, edge computing, and the Internet of Things (IoT), cloud-based and intelligent pass management platforms have gradually become key solutions to these issues. This paper leverages the integrated advantages of cloud and edge computing to propose an innovative design for a nationwide airport restricted area pass management platform. The paper provides a comprehensive analysis of the platform's architecture design, key technologies, and practical application outcomes, aiming to offer valuable references and insights for the intelligent and secure management of airports nationwide.

2. The Application of Cloud Computing and Edge Computing in Pass Management

(1) Cloud Computing

As a technology based on centralized resource management, cloud computing provides powerful computational capacity and data storage support for the pass management platform[2]. Through cloud computing, the platform can achieve centralized management of pass data, including functions such as data storage, identity verification, and permission allocation, thereby improving the standardization and regulation of management processes. However, cloud computing faces limitations in handling high concurrency demands and real-time scenarios at airports due to network transmission delays and bandwidth pressure. These challenges become particularly evident in complex scenarios involving frequent personnel movement and widely distributed areas within airports[3].

(2) Edge Computing

Edge computing, by offloading computational and data processing tasks to edge nodes near the data source, can effectively reduce data transmission delays and improve real-time responsiveness. In airport restricted area pass management, edge computing nodes can be deployed at critical locations such as airport entrances and security checkpoints to enable localized pass verification and permission management[4]. The introduction of edge computing not only reduces dependence on the cloud but also enhances the efficiency and security of data processing. However, the computational resources of edge nodes are relatively limited, necessitating cloud-edge collaboration to achieve more comprehensive functionality.

3. Demand Analysis of the Nationwide Airport Restricted Area Pass Management Platform

(1) Real-Time Requirements

Airport restricted area pass management has extremely high demands for real-time performance, especially in processes such as identity verification, permission validation, and abnormal alert handling. For instance, during peak hours, security checkpoints need to verify passes within milliseconds to ensure efficient and safe personnel passage. Traditional cloud computing struggles to meet this requirement due to data transmission delays, whereas the localized processing capabilities of edge computing provide an effective solution to the real-time challenge.

(2) Data Security and Privacy Requirements

Pass data in airport restricted areas involves sensitive information such as personal identity details and access permissions, making data security and privacy protection particularly critical. In a cloud computing environment, data is exposed to risks of cyberattacks and breaches. Edge computing, by processing data locally, reduces the frequency of data transmission and thus minimizes the risk of exposure. However, edge nodes also face challenges such as physical device security and access control[6]. It is necessary to establish stringent security mechanisms to ensure data safety throughout its entire lifecycle.

(3) Scalability Requirements

With seasonal fluctuations and long-term growth in airport passenger traffic, the nationwide airport restricted area pass management platform must possess excellent scalability to meet the diverse requirements of different airports and adapt to future development trends. The elastic scalability of cloud computing offers significant advantages in handling large-scale data growth, while the dynamic deployment and resource scheduling of edge computing nodes are equally critical to ensuring the platform's sustainable development.

4. Cloud-Edge Integrated Architecture Design

(1) Overall Architecture

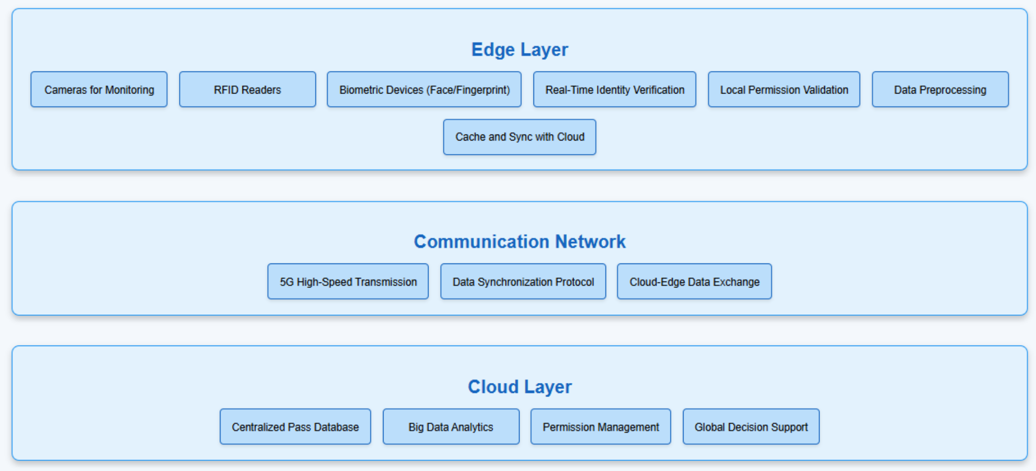

Figure 1. Overall Architecture

To meet the requirements of efficiency, security, and scalability in airport restricted area pass management, this paper proposes an architecture design optimized through the integration of cloud computing and edge computing. The architecture consists of three layers: the edge layer, the cloud layer, and the communication network layer.

Edge Layer: Deployed at key areas of airports, edge computing nodes are responsible for local data collection and rapid processing of pass-related information. For example, devices such as cameras and RFID card readers collect pass information in real time, while the edge nodes conduct preliminary verification and permission checks.

Cloud Platform: The cloud platform provides large-scale data storage, in-depth analysis, and global management functions. For instance, it supports cross-airport pass data correlation analysis and the optimization of permission allocation strategies.

Communication Network Layer: A combination of 5G networks and wired networks ensures stable and efficient data transmission between edge nodes and the cloud. This setup is designed to meet real-time requirements in high-concurrency scenarios.

(2) Data Processing Workflow

The data processing workflow of the pass management platform consists of three stages: data collection, preliminary analysis, and in-depth analysis. Edge nodes use sensing devices to collect pass information in real time and perform data preprocessing, such as feature extraction and format conversion. Edge nodes handle high-priority tasks locally, such as real-time identity verification and permission checks. Critical data is then uploaded to the cloud for further processing. The cloud aggregates and deeply analyzes cross-regional and cross-node data. By leveraging big data and artificial intelligence algorithms, the platform identifies potential security risks and optimizes permission management strategies.

5. Key Technologies and Implementation Methods

(1) Cloud-Edge Collaborative Scheduling Algorithm

The cloud-edge collaborative scheduling algorithm is a key technology for enabling efficient collaboration between cloud computing and edge computing. Its goal is to allocate tasks to edge nodes or the cloud based on task characteristics, resource availability, and real-time requirements, thereby optimizing system performance and resource utilization while meeting the strict real-time requirements of the airport restricted area pass management platform.

This study employs a priority- and resource-aware scheduling algorithm, with the following steps:

When a task arrives, its priority is determined first. Priority is classified based on task type and urgency. Tasks directly related to personnel passage and airport security, such as real-time identity verification and permission validation, are assigned high priority. Non-critical tasks with less stringent real-time requirements, such as data statistics analysis or historical record queries, are assigned low priority.

The resource status of edge nodes is assessed, including key metrics such as CPU utilization, memory usage, and network bandwidth consumption.

If edge node resources are sufficient and the task is high priority, the task is assigned to the edge node for local processing, leveraging its low-latency advantage to meet real-time requirements. For example, during identity verification at a security checkpoint, the edge node processes the task using local resources, reducing data transmission time and improving passage efficiency.

For medium-priority tasks, both the edge node and cloud load conditions are considered. If the edge node's load is light and processing the task does not affect high-priority tasks, the task is executed locally at the edge node. Otherwise, it is forwarded to the cloud for processing. For example, some permission validation tasks are processed locally if edge resources are available, or sent to the cloud if resources are constrained.

Low-priority tasks and tasks requiring significant computational resources and complex data analysis, such as risk prediction based on big data and long-term permission strategy optimization, are directly assigned to the cloud. The cloud, with its powerful computational capabilities and massive data storage, efficiently handles such tasks.

To further optimize task allocation, a dynamic adjustment mechanism is introduced. Resource usage at edge nodes and the cloud is monitored periodically, and task allocation is adjusted in real-time based on load fluctuations.

For instance, when an edge node is heavily loaded, some medium-priority tasks are transferred to the cloud. Conversely, when the cloud is heavily loaded, tasks that can be processed at the edge are assigned to edge nodes.

Additionally, task execution history is analyzed to predict future task volumes and resource demands, enabling proactive resource allocation to prevent system congestion.

By utilizing this cloud-edge collaborative scheduling algorithm, tasks are allocated effectively between edge nodes and the cloud. High-priority real-time tasks are processed rapidly, complex tasks are executed efficiently, and system load is balanced, thereby enhancing overall system performance.

(2) Security Mechanism

The security mechanism aims to establish a comprehensive, multi-layered security protection system for the airport restricted area pass management platform, ensuring the security of pass data throughout its transmission, storage, and usage processes.

SSL/TLS protocols are used to encrypt data communication between edge nodes and the cloud. During the connection establishment phase, both parties negotiate encryption algorithms and keys through a handshake protocol to ensure the confidentiality and integrity of data transmission. For example, when edge nodes upload identity verification data or the cloud issues permission update instructions, all data is transmitted within an SSL/TLS encrypted channel, effectively preventing network attacks and eavesdropping.

Both the cloud and edge nodes use encryption algorithms to store data securely. Sensitive data, such as personal ID numbers and biometric information, is encrypted using the AES (Advanced Encryption Standard) algorithm and stored as ciphertext. Only authorized users with decryption keys can access and restore the data. Additionally, blockchain technology is integrated for distributed storage and verification of critical data, such as pass issuance records and important operation logs. The immutability of blockchain ensures the authenticity and integrity of the data. Each data record is stored in a blockchain block and linked through hash algorithms to form an immutable chain, where any tampering attempts can be detected by network nodes.

Strict identity authentication is enforced for edge computing nodes and devices accessing the platform. Digital certificate technology is used to issue a unique digital certificate to authorized devices. When devices attempt to connect, they must present their certificate for identity verification. Only authenticated devices are allowed to communicate and interact with the platform, preventing unauthorized devices from accessing data or launching attacks.

A role-based access control (RBAC) model is widely applied. Permissions are assigned based on user roles (e.g., airport management personnel, security checkpoint staff, passengers) and responsibilities. Airport management personnel can manage the entire lifecycle of passes. Security staff are restricted to verifying passes and handling exceptions. Passengers can only view their own pass information.

Access control strictly limits users' access to data and functions, ensuring that only authorized actions are allowed, thereby preventing unauthorized access and data leaks.

The platform includes a security auditing system to monitor and record all operations in real time, including user logins, data access, and permission changes. Audit logs are periodically analyzed to identify potential security threats and unauthorized actions, enabling timely measures to enhance security protections.

By implementing these security mechanisms, the platform ensures robust protection for pass data, combats unauthorized access, and maintains the integrity and confidentiality of the system.

6. Conclusion

Through the implementation of these key technologies, cloud computing and edge computing achieve deep integration within the airport restricted area pass management platform, establishing a solid technical foundation for the platform's efficient and secure operation.

This paper proposes a nationwide airport restricted area pass management platform architecture based on cloud-edge integration. Experiments and real-world cases have validated its significant advantages in terms of real-time performance, security, and scalability. In the future, with the continued development of mobile communication networks, quantum computing, and artificial intelligence technologies, the application prospects of the cloud-edge integration architecture in smart airport management will become even broader.

Acknowledgments

The authors would like to express their sincere gratitude to their leaders and colleagues for their invaluable guidance, support, and encouragement throughout the course of this work. Their expertise, collaboration, and dedication were instrumental in overcoming challenges and achieving the goals of this project. The authors deeply appreciate their trust, valuable insights, and unwavering belief in the success of this endeavor.

References

[1] Silvianda S, Sihombing I M, Erma Z. Legal review of airport pass service at the airport authority office in region ii medan when entering the security restricted area[J]. Legal Brief, 2023, 11(6): 3574-3583.

[2] Sadeeq M M, Abdulkareem N M, Zeebaree S R M, et al. IoT and Cloud computing issues, challenges and opportunities: A review[J]. Qubahan Academic Journal, 2021, 1(2): 1-7.

[3] Lyu Z, Luo J. A surveillance video real-time object detection system based on edge-cloud cooperation in airport apron[J]. Applied Sciences, 2022, 12(19): 10128.

[4] Kong L, Tan J, Huang J, et al. Edge-computing-driven internet of things: A survey[J]. ACM Computing Surveys, 2022, 55(8): 1-41.

[5] Liu X, Wang Q, Zou C, et al. Edge intelligence for smart airport runway: Architectures and enabling technologies[J]. Computer Communications, 2022, 195: 323-333.

[6] Alabsi M I, Gill A Q. A review of passenger digital information privacy concerns in smart airports[J]. IEEE Access, 2021, 9: 33769-33781.