applied sciences

MDPI

Article

An Access Control Framework for Multilayer Rail Transit Systems Based on Trust and Sensitivity Attributes

Xin Geng [1,2,*], Yinghong Wen [1], Zhisong Mo [3] and Yu Liu [2]

[1] Institute of Electromagnetic Compatibility, Beijing Jiaotong University, Beijing 100044, China; yhwen@bjtu.edu.cn
[2] China Railway Information Technology Group Co., Ltd., Beijing 100844, China; liuyu2@sinorail.com
[3] China State Railway Group Co., Ltd., Beijing 100038, China; mozhisong@hotmail.com
* Correspondence: 12111054@bjtu.edu.cn

Abstract: The construction of multilayer rail transit systems is a necessary way to realize "modern metropolitan areas on rail", improve resource sharing, and increase travel services, where data integration is of utmost importance. To break data silos and realize data flow between different rail systems, a fine-grained access control framework is proposed in this paper. Through categorical and hierarchical schemes, a universal security scale is established for cross-domain data resources. Based on this, a trust and sensitivity attribute-based access control (TSABAC) model is put forward to describe the characteristics of the access control process. Furthermore, the method of policy integration is discussed, as well as the solution to the policy incompatibility problem, due to cross-domain interaction. As shown in practical application and simulation analysis, this framework can meet the requirements of security and granularity. This research is of great significance for promoting the high-quality development of urban agglomerations and metropolitan areas, and improving the quality and efficiency of rail transit.

Keywords: multilayer rail transit system integration; access control framework; conflict resolution; policy composition; ABAC

Citation: Geng, X.; Wen, Y.; Mo, Z.; Liu, Y. An Access Control Framework for Multilayer Rail Transit Systems Based on Trust and Sensitivity Attributes. *Appl. Sci.* **2023**, *13*, 12904. https://doi.org/10.3390/app132312904

Academic Editor: Paolino Di Felice

Received: 14 October 2023
Revised: 10 November 2023
Accepted: 15 November 2023
Published: 1 December 2023

1. Introduction

With the continuous expansion of the rail transit network and the continuous improvement of rail transportation services in China, the spatial and temporal distances within the metropolitan area have been greatly reduced, which has effectively promoted the transformation and upgrading of regional industries and accelerated the cultivation, development, and growth of urban clusters [1]. At the same time, since the rise of urban clusters has entered the stage of high quality development, the needs for transportation services are presenting new characteristics, which bring both challenges and opportunities for the development of rail transit. China has been promoting the development of a multilayer rail transit system through top-level design, explicitly stating the goal of building "modern metropolitan areas on rail" and carrying out the "four-network integration" of trunk railways, intercity railways, suburban railways, and urban rail transit. Therefore, in the context of gradually integrating and coordinating multiple rail transit modes after the road network reaches a certain scale, the concept of synergetic regional rail transportation and services has emerged [2]. Aiming to leverage the advantages of a regional rail transit network and fully tap into its transport capacity, the multilayer rail transit integration raises standards of service, provides strong support for urban cluster construction, and promotes the intelligence of rail transit with the metropolitan area expanding.

Currently, data of the four rail transit networks are often stored and used separately, resulting in data silos where the data cannot be smoothly connected or interact with each other. To achieve true "four-network integration", data integration is of utmost importance [3]. It involves breaking down the barriers between the four rail networks and enabling data flow

across different entities. However, such cross-entity, cross-responsibility, and cross-domain data interactions can bring about severe security issues within enterprises and may even lead to the leakage of personal privacy or even significant national data. From the point view of the SRIDE Threat Model, the impropriate access to information resources may lead to tampering and information disclosure. For example, modification of automatic train supervision system data and configuration files may cause service degradation or termination, resulting in impact on security functions; collecting by means of maintenance tools (port scanning, network packet capture tools, etc.) or additional hardware (eavesdropping, monitoring of transmitted signals) may also cause severe data disclosure.

Since access control is one of the most effective technical means to prevent the above issues, an effective framework for multilayer rail transit data interactions is important to protect the privacy of individuals and railway business resources [4]. However, due to the enormity and complexity of the rail transit systems, current structure of control over data exchange processes is insufficient. Generally, each rail system has its own access control scheme, so as to protect the data flow within the system. Thus, the key point of cross-domain interaction is to combine different policy schemes and realize fine-grained access according to the principle of least privilege. To achieve the global access control, it first requires the universal evaluation on the security characteristics of an access request, then different policy sets should be integrated with a combination algorithm. In the case of incompatible problems due to various models, conflict resolution is ought to be executed.

There has been some research on access control strategies in rail transit systems. A mandatory access control system for application security was proposed for gateway devices in railway information systems [5]. A fine-grained access control scheme of a railway cloud platform based on mandatory access control and zero trust access control policy was put forward in the framework of a network security protection system for a railway cloud platform according to the baseline of classified protection of information system security [6]. A collaborative design method of subway comprehensive pipelines is based on role-based access control and a building information model, to realize information sharing and control the coordination of data exchanges and activities among different design professionals [7]. Recently, a block-chain data access control model has been developed based on attribute elements to ensure the access security and storage security of data assets during the sharing process [8]. In addition, a dynamic real-time credibility access control method has been put forward based on zero trust and continuous authentication with trust evaluation carried out throughout the access control process [9].

The research above has realized flexible and scalable access control of information resources, but there are still some shortcomings for the scenario of multilevel rail transit systems. Firstly, seeing that the diversity of different rail business, there is not an effective and universal assessment of data security, not only on a macroscopic perspective of rail information, but also on a microscopic perspective of data exchange performance. Secondly, the control model should be compatible with current schemes, as well as the combination algorithm. Finally, to cover different secure domains, policy conflict problems ought to be considered.

Therefore, this paper proposes an access control framework for data integration in multilayer rail transit systems based on the trust and sensitivity attributes. The structure of the paper is as follows: Section 2 formulates and analyzes the characteristics of data to share integration in rail transit systems and proposes the access control scheme based on ABAC. To achieve fine-grained data control, Section 3 raises an attribute-based access control strategy by defining dynamic security attribute labels such as data sensitivity and user trust. Section 4 introduces a cross-domain hybrid access control model, which achieves compatibility between different access control strategies through access control detection and resolution. Section 5 demonstrates the feasibility and practicality of the framework through practical examples. Finally, the conclusion summarizes the entire paper.

2. Problem Formulation

2.1. Demand for Collaborative Information in Multilayer Rail Transit System Integration

With the rapid development of the rail transit industry, there is a demand for solution and technology on the allocation of multilayer regional capacity resources, optimization of overall transportation organization, collaborative and comprehensive safety assurance, and integrated passenger information services. Therefore, research focusing on single-mode operation has become increasingly inadequate to adapt to the upcoming situation. Here are some specific manifestations. For passenger flow prediction, under multilayer network operations, the spatiotemporal characteristics of multiple level overlapping passenger transport will change, making the existing flow prediction models difficult to apply. For train operation organization, since different modes are interdependent and mutually constrained, existing methods are no longer suitable for the requirements of regional collaborative operations, such as hub transfers, capacity allocation, and dispatching. For resource utilization, the comprehensive utilization and resource sharing of network system facilities will be different from the previous method of single-mode operations; regional rail transit operates different modes independently but connects them through physical hubs, especially when it comes to the coordination and command of the safety assurance system in emergency situations. For passenger information services, it includes more accurate information services, convenient access, and intelligent query retrieval based on natural language interaction, in terms of intelligence, comprehensiveness, flexibility, interactivity, transparency, and cost-effectiveness.

The realization of collaborative scenarios depends on data resource exchange in multilayered rail transit systems. In general, information requested can be divided into three forms: basic information, business information, and comprehensive information. Basic information refers to the data, graphics, attributes, and coding resources that can reflect the basic situation of railway transportation. Business information refers to the data and graphics that support the operation of railway business information systems and participates in railway business operation related to business. Comprehensive information refers to the management, control, and comprehensive decision information formed during the operation of a business system due to the requirements of business applications through the information comprehensive analysis and calculation of relevant business models. According to previous research and literature reviews [10], the information requested by main businesses is shown in Figure 1.

2.2. Categorical and Hierarchical System for Integrated Data in Multilayer Rail Transit Systems

The interaction of data across different systems makes it difficult to determine a universal security scale. Therefore, it is necessary to construct a classification and grading system for integrated data in multilevel rail transit systems based on actual business requirements. Based on "Guidelines for Classification and Grading of Railway Data (Interim)" by the China Railway Corporation, the categorical and hierarchical system for data integration in multilevel rail transit systems is proposed, consisting of three dimensions: data category, security hierarchy, and lifecycle, as shown in Figure 2.

A. Categorization of Rail Transit Data

The categorization of rail transit data starts with the analysis of relevant information systems, i.e., the business domain to which the information system belongs, as well as the primary and secondary subcategories of the business. Once the business domain of the information system is determined, the data are further divided into subcategories at the primary and secondary levels, until the smallest data class is reached.

B. Hierarchization of Rail Transit Data

The hierarchization is the process of assigning security levels to data based on its importance and sensitivity. As for railway data, they are a comprehensive assessment according to the impact factors (including the national security, public interests, individual legitimate rights, and organizational legitimate rights), as well as the degree of impact

(ranging from no harm, slight harm, general harm, to severe harm). The basic levels of data, from low to high, are general data, important data, and core data. General data can be further subdivided into four grades for fine-grained integration and interaction, while core data and important data should be included in the important data catalog for focused protection.

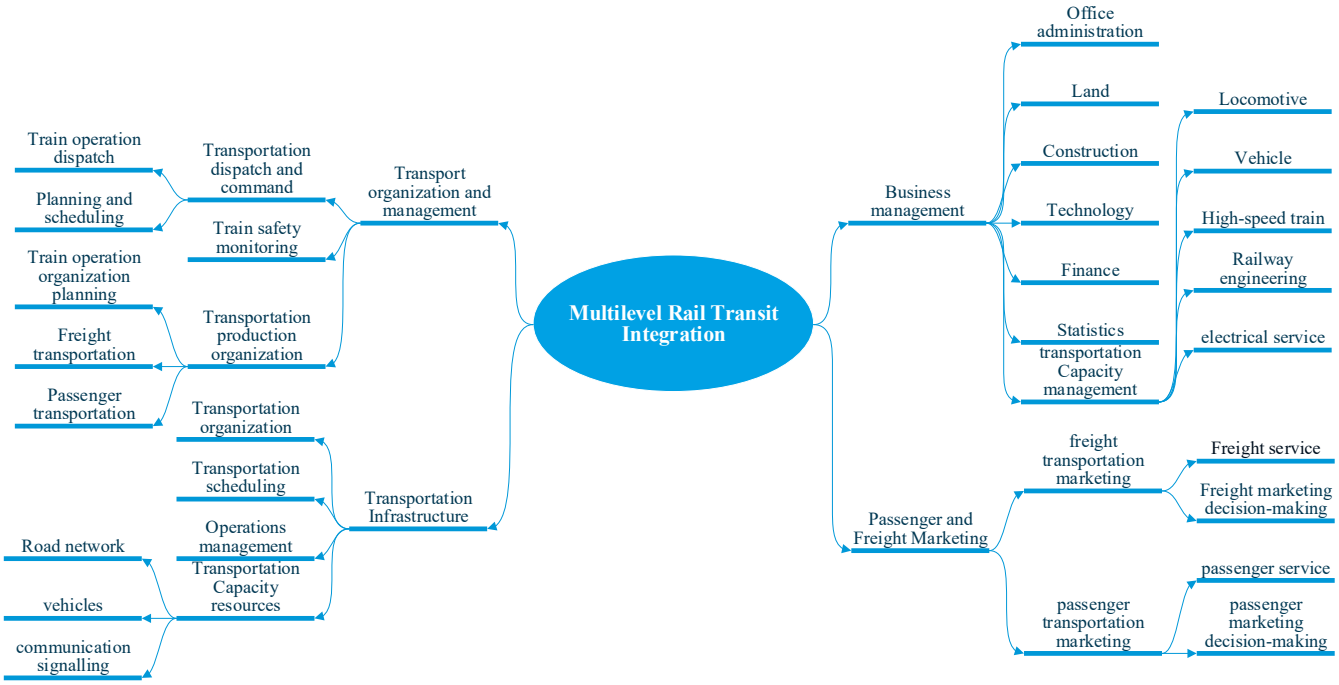


Figure 1. Summary of information requested in multilayer rail transit systems.

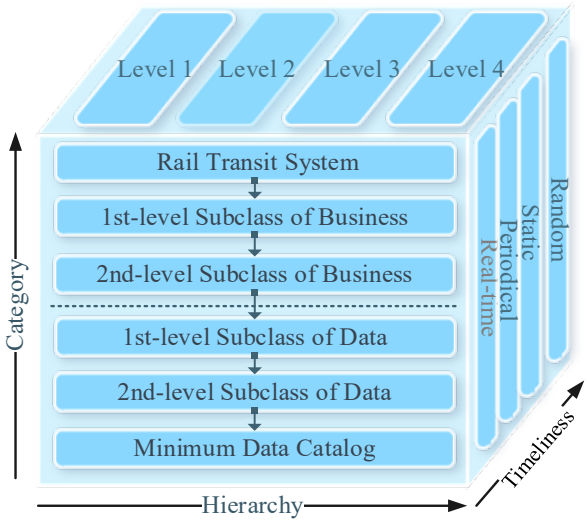


Figure 2. Diagram of categorical and hierarchical system for integrated data.

C. Lifecycle of Rail Transit Data

The lifecycle describes the phased changes and patterns of data from a temporal perspective. The data lifecycle can be divided into six stages: data collection, data transmission, data storage, data processing, data exchange, and data destruction [11]. In the lifecycle, the categorization and hierarchization of data may change over time, policies, or business scenarios. Particularly, some information is generated and varied throughout the train operation, requiring real-time delivery to relevant information systems, such as train operation records, on-time performance, train safety monitoring, and disaster safety

monitoring. Some information belongs to relatively static data, such as basic data of station, transportation plans, and statistical data, which can interact with other systems periodically as needed [12]. Therefore, it is necessary to regularly review and adjust the category and hierarchy of data resources.

The categorical and hierarchical systems provide a basis for fine-grained and full lifecycle security control of rail transit data, which is of great significance for balancing data security and business requirements [13]. By classifying and grading data resources, the security levels and protection requirements of the data can be clearly defined. A typical categorization and hierarchization example is shown in Table 1.

Table 1. Typical categorization and hierarchization of rail transit data.

Data Item	Category			Hierarchy	Timeliness
	1st-Level Subclass of Business	2nd-Level Subclass of Business	Subclass of Data		
Bridge location	Management	Construction	Bridge construction	2	Static
Tunnel length	Management	Construction	Tunnel construction	2	Static
Slope rate	Management	Construction	Roadbed construction	2	Static
Locomotive inspection and repair	Management	Equipment	Locomotive and vehicle	4	periodical
Operating status of computer-interlocking system	Management	Monitoring	Fixed facility monitoring	3	Real-time
Train operation safety monitoring information	Management	Monitoring	Mobile facility monitoring	3	Real-time
Slope displacement monitoring	Management	Monitoring	Disaster monitoring	3	Real-time
Train electricity consumption	Production	Train	Electric information	2	Periodical
Balise inspection/service logs	Production	Operation and maintenance	Facilities maintenance	3	Periodical
Statistics of ticket reservation	Production	Dispatch	Passenger flow forecast	1	Real-time
Freight train formation plan	Production	Dispatch	Train operation plan	4	Real-time
Train speed and position measurement	Production	Train control	Operational control	4	Real-time
Passenger ID information	External	User	Passenger	4	Periodical
Organization code	External	User	Supplier	2	Periodical
Passenger throughput	External	Network	Network traffic	2	Periodical
Passenger arrivals	External	Passenger flow	Transfer station	4	Periodical

2.3. Access Control Framework for Multilayered Railway Systems

Since the concept of an access control matrix was proposed, many access control models have emerged, such as discretionary access control (DAC), mandatory access control (MAC), usage control (UCON), task-based access control (TBAC), role-based access control (RBAC), and attribute-based access control (ABAC). They each have their own characteristics and have been widely used in different environments. DAC excels in its flexibility in authorization. MAC demonstrates outstanding performance in system security

and confidentiality. RBAC has advantages in terms of intuitive understanding, flexible authorization, separation of duties, and descriptive capabilities. ABAC performs well in descriptive capabilities and access control granularity.

To select a suitable access control framework for the data interaction scenarios in rail transit, we need to quantitatively compare the performance of these widely used models. So far, there is no unified quantitative evaluation standard in the industry to measure the effectiveness and quality of access control models. In this paper, we mainly consider the basic capabilities from four aspects: control capability, operating cost, coverage, and usability. Specifically, we used a set of indicators to measure the performance of access control models, namely criteria = {granularity, expressiveness, complexity, scalability, compatibility, flexibility, security}, where granularity and expressiveness are suitable criteria to measure the control capability, complexity shows the operating cost, scalability, and complexity reflecting the coverage, while flexibility and security refer to the usability. As for the application scenarios of the multilayer domain rail transit system, the security is the most significant since some data concerns national and public safety, and the control capability and coverage come posteriorly to achieve universal access control. Therefore, the corresponding weights were set as w = {0.2, 0.1, 0.05, 0.1, 0.2, 0.1, 0.25}. According to previous research [14] and inherent attributes of the models mentioned above, each indicator is scored from 1 to 4, based on the performance of these models in a cross-domain environment. The better the performance, the higher the score. Therefore, the global assessment is expressed as $\text{Assessment}_{gobal} = \sum_{i \in Criteria} w_i Value_i$, as shown in Table 2.

Table 2. Performance comparison of major access control models in cross-domain environments.

Model	Granularity	Expressiveness	Complexity	Scalability	Compatibility	Flexibility	Security	Assessment
DAC	1	1	4	2	1	3	1	2.05
MAC	1	1	4	1	1	1	4	2.1
RBAC	3	3	3	3	3	2	2	3.05
ABAC	4	4	1	4	4	4	3	3.4
TABC	2	2	2	2	3	4	2	3.2
UCON	4	3	1	3	3	2	1	2.9

As can be seen from Table 2, the attribute-based model is more suitable for a large-scale cross-domain network environment than the others. However, in the process of data fusion of a multilayer domain rail transit system, the independence of the policies defined in each control domain causes lots of compatibility issues between domains, and results in the problem of semantic inconsistency and policy conflict. The basic elements of access procedure consist of subject, object, condition, and operation, which are described with attributes. The concept of attribute can express all the access control models and provide a universal policy description model. Based on a typical ABAC model, a fine-grained access control architecture for data integration in multilayer rail transit scenarios is proposed, to realize cross-domain secure sharing of information resources, as shown in Figure 3. The access process is as follows: the policy enforcement point (PEP) receives the original access request (AR), and builds an attribute-based access request (AAR) using the attribute information stored in attribute authority (AA) according to AR, where significant attributes, i.e., category, hierarchy, trust and sensitivity, are assigned as a supplement to describe the global security level of the AAR. The AAR describes the subject, object, action and condition properties, and the PEP passes the AAR to the PDP as well as the policy administration point (PAP), and PAP should determine the permission of AAR. As for the cross-domain policies, to integrate policies from different rail transit systems, we put forward unified formalization and combination algorithms. In addition, policy detection and resolution are performed based on the universal policy model, in case of access policy incompatibility

issues. PAP passes the permission to PEP, and PEP executes the access decision result to finally determine the access permission of the user.

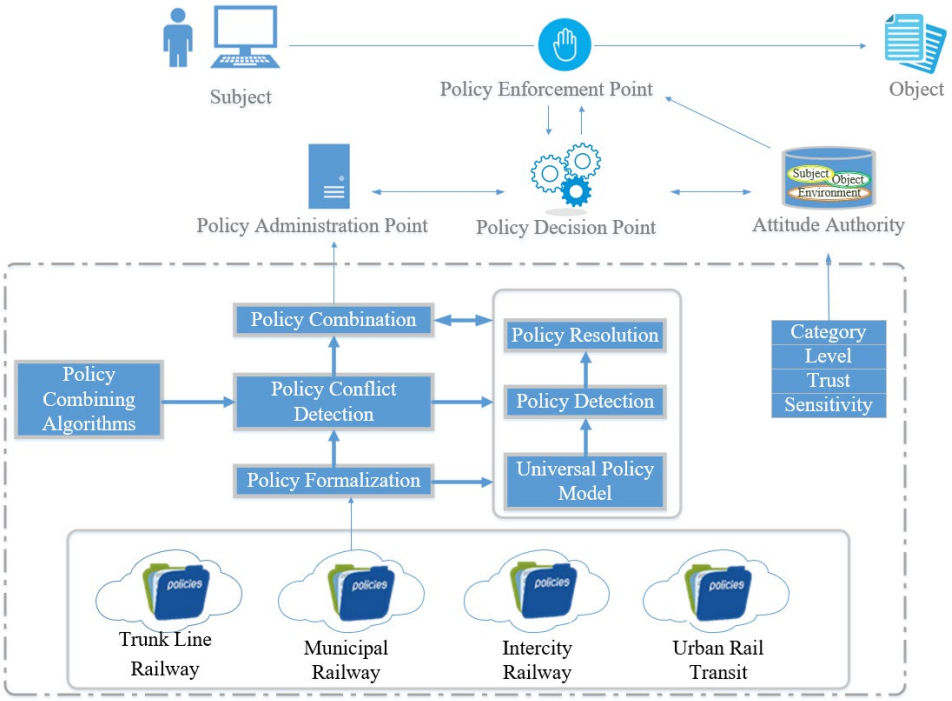


Figure 3. Access control framework for data sharing in a multilayer rail transit system based on ABAC.

3. Access Control Policy Combination Method for Data Fusion in Railway Traffic Systems

In this section, we first introduce the attributes of object sensitivity and subject trust into attribute-based access control policies to reflect the performance of entities such as subjects and objects during data exchange. The access permission of the subjects is dynamically adjusted by these attribute values; thus, the authorized access of some malicious nodes is prevented and the safety of rail transit data assets is protected. Then, the model of trust and sensitivity attributes trust and sensitivity attribute-based access control (TSABAC) is defined based on trust and sensitivity. Finally, the algebra form of policy composition is defined.

3.1. Object Sensitivity

Data categorization and hierarchization are based on a qualitative analysis of the data content, which is relatively static and cannot reflect the influence of data in the case of malicious access. Therefore, it is necessary to raise a sensitivity indicator to dynamically evaluate the impact of an object on the other entities in the whole system through previous interactions. In a multilayer rail transit system, we take a data table as the basic unit of access control object, and its importance depends on utilization and correlation, which are evaluated based on information entropy.

A. Utilization

Utilization refers to the frequency at which an object is accessed externally. By comparing the frequency of all objects, it can be observed that core business data are typically accessed more frequently with higher utilization, so the consequence is severer in the case of misuse, indicating higher sensitivity. Let K_i represent the set of subjects accessing object i

at time period t, and function $count(K_i)$ represents the number of elements in set K_i. The connectivity information entropy of i is defined as I_i^c:

$$I_i^c = -\sum_{j \in K_j(t)} \frac{1}{count(K_j)+1} lb \frac{1}{count(K_j)+1} \tag{1}$$

Let F_{ij} be the number of interactions between subject j and object i. The interaction frequency information entropy of i is defined as I_i^f:

$$I_i^f = -\sum_{j \in K_j} \frac{F_{ij}}{\sum\limits_{k \in K_i} F_{ik}+1} lb \frac{F_{ij}}{\sum\limits_{k \in K_i} F_{ik}+1} \tag{2}$$

Therefore, the data utilization H_i^u is the product of its connectivity information entropy I_i^c and the interaction frequency information entropy I_i, given by:

$$H_i^U = I_i^c * I_i^f \tag{3}$$

B. Correlation.

Object correlation refers to the frequency at which an object is associated with other objects. If subject k accesses both objects i and j during time period t, i.e., $K_{ij} = K_i \cap K_j \neq \phi$, then objects i and j are considered to be correlated and form a path R_{ij} with subject k, which is constructed by the order of accessed objects by subject k. A path may pass through one or more objects apart from i and j, thus the correlation information entropy between objects i and j is:

$$H_{ij}^C = \sum_{k=1}^{N} \frac{\theta + H_i^U}{\prod\limits_{m \in R_k} (\theta + H_m^U)} \tag{4}$$

where N refers to the number of paths between i and j, and θ represents the influence of the network environment, assuming that the entity is not connected to others and has its inherent influence when calculating indirect influence. Here, θ is set to 1 [15].

The sensitivity of an object should be evaluated based on both its utilization and correlation:

$$S_{ij} = \alpha H_i^U + (1-\alpha) H_{ij}^C \tag{5}$$

where $\alpha \in [0, 1]$ is the coefficient for the influence of utilization on the total sensitivity. For any new entity, its correlation with other entities is not of much significancy, thus we have $\alpha = 1$. If the accessing the subject receives feedback information due to previous malicious behavior, its trust will be decreased. For a core business object i with extremely high secure hierarchy, its utilization may be low. However, as the data interaction proceeds, the sensitivity of its associated objects is experiencing rapid increase due to frequency related, so its correlation is quite significant, indicating a non-negligible sensitivity on the whole.

3.2. Subject Trust

The trust in an access control model refers to the rating given by the participating entities in the current request or session. The more frequent and positive the interaction between the requesting subject and the target object during the authorization process, the higher the trust value between them. Trust consists of direct trust and recommendation trust.

Although the performance of the accessing subject is evaluated based on different standards in different environments specifically, the general criteria include security attributes, reliability attributes, and performance attributes. Security attributes refer to the average number of illegal connections, the average number of scans on important ports, the average number of unauthorized attempts, the average number of virus carriers, and the average number of attacks. Reliability attributes consist of the average user error rate, the average user packet loss rate, the average connection establishment failure rate, and

the average service success rate. Performance attributes include the average user IP packet response time, the average throughput, the average IP packet transmission delay, and the average storage resource occupancy rate [16]. For a given attribute index $B_k \in [0, 1]$ and the corresponding weight coefficient t_k, where $t_k \in [0, 1]$ and $\sum t_k = 1$, the trust between i and j is $D_{ij} = \sum_k t_k B_k$, ranging from 0 to 1.

A. Direct trust.

Direct trust refers to the rating given by a target object. For requesting subject i and object j, direct trust of the *k-th* participation is evaluated based on their direct interaction or session, denoted as ${DT^k}_{ij}$. To reflect the behavior of i in real time, time decay is taken into account, thus ${DT^k}_{ij}$ can be represented in a recursive form as:

$$DT_{ij} = \tau DT_{ij}^{k-1} + \sigma(1-\tau)DT_{ij}^{k}, k \geq 1 \tag{6}$$

where ${DT^0}_{ij}$ represents the initial value, and is set to 0.5, indicating a moderate level of trust. The time decay factor $\tau \in [0, 1]$ describes the influence of previous interactions on the current trust value. A larger α indicates a higher weight of historical trust in the calculation, and $\tau = 0$ indicates that the previous trust value is not considered. The success rate of historical interactions is represented by $\sigma = \sqrt{N_{ij}/(M_{ij}+1)}$, where N_{ij} represents the number of successful interactions and M_{ij} represents the total number of historical interactions. The index σ aims to incentivize entities to maintain a high trust level gained before, preventing dishonest or malicious behavior by the subject.

B. Recommendation trust.

Recommendation trust ${RT^k}_{ij}$ refers to the trust between two entities i and j, obtained through recommendations from a third entity k with whom both i and j have interacted. To prevent malicious entities from exaggerating or defaming behaviors during the evaluation process, as well as to avoid external interference on the accessing entity, the trust of entity k towards entity i is used as the recommendation trust coefficient. So ${RT^k}_{ij}$ is represented as:

$$RT_{ij} = \frac{\sum\limits_{k} DT_{kj} DT_{ik}(x_i, x_k) N_{ik}}{\sum\limits_{k \in K_i} N_{ik}} \tag{7}$$

The trust T_{ij} of the accessing subject is mainly calculated based on the relevant direct trust and recommendation trust in the policy:

$$T_{ij} = \beta DT_{ij} + (1-\beta)RT_{ij} \tag{8}$$

where $\beta \in [0, 1]$ represents the influence of direct trust on the total trust. When $\beta = 1$, it indicates that the entity is newly added to the access control system, so the recommendation trust is not considered. If the accessing subject receives feedback information due to previous malicious behavior, its trust will be decreased. When the trust of the subject decreases to a certain level, it indicates that the entity is a malicious node and its trust cannot be recovered for a long period of time.

3.3. Policy of TSABAC

A TSABAC access policy has three main components [17]: a target, a conditionand an effect. The target defines a set of subjects, resources, and operations that the rule applies to; the condition specifies restrictions on the attributes in the target and refines the applicability of the rule; the effect is either permit, in which case we call the rule a permit rule, or deny, in which case we call it a deny rule. In multilayer rail transit systems, the subject refers to the active entities such as users and processes that request access, and $SA = (sa_1, sa_2, \ldots, sa_m)$ is the subject attribute set. The object refers to the passive entities in the information system that are being accessed, including data, devices, networks, etc., and $OA = (oa_1,$

$oa_2, \ldots, oa_n$) represents the object attribute set. The operation refers to the access request actions performed by the subject on the object, such as reading, writing, editing, deleting, copying, searching, and modifying. The condition represents dynamic factors independent of the subject and object, and plays an important role in access control decision-making, such as time, geographical location, and network performance, and $CA = (ca_1, ca_2, \ldots, ca_k)$ represents conditional attribute set. To characterize the dynamic authorization relationship between the subject and the object, the model of TSABAC policy is:

$$pol = < SA,\ OA,\ CA,\ T,\ S, OP, eff > \tag{9}$$

Meanwhile, to express a specific access request, attribute authorization items can be formally defined as:

$$att = (SA, OA, CA, T, S, OP) \tag{10}$$

If a request satisfies both the rule target and rule condition, the policy is applicable to the request and yields the decision specified by the effect element; otherwise, the policy is not applicable to the request and yields the decision not applicable. Thus, four-valued logic is used to describe the effect of an access request. Re $\in \Sigma$ = {0(deny), 1(permit), $\perp$(not applicable), and $\top$(conflict)}. The essential difference between four-valued logic and classical two-value logic is whether "there is information which supports *att*" is equivalent to "there is no information which opposes *att*". This definition can intuitively represent the two states of information and the four states of results integration between the evaluation results [17].

If the attribute tuples in two attribute authorization items are exactly the same, the attribute authorization items are called compatible. Otherwise, the extended formation is proposed to maintain consistency in attribute authorization items. When it comes to synthesizing two or more attribute authorization items in the access control policy, if there is no corresponding attribute value for a certain entity attribute, we use Δ to represent the null value. In the process of synthesis, this value is considered non-existent and does not participate in any calculations. Therefore, different policy calculations can be implemented by extending the attribute authorization items. For example, if we have two entity attribute authorization items att_1 = {(level > 2), (T $\geq$ 0.4)} and att_2 = {(level > 3), (S $\geq$ 0.8)}, the extended versions would be att'_1 = {(level > 2), (T$\geq$ 0.4), Δ_1} and att'_2 = {(level > 3), Δ_2, (S $\geq$ 0.8)}.

Theorem 1. *Using ATT to represent the set of extended attribute authorization items and FA = {f_i} is the set of extended binary operation on each attribute tuple, so (ATT, FA) forms an algebraic system.*

Proof. For $\forall$att $\in$ ATT, let att' and att'' be the extensions of att and att', respectively, denoted as att' = {<$sa_1, sa_2, \ldots, sa_m$>, < $oa_1, oa_2, \ldots, oa_n$ >, < $ca_1, ca_2, \ldots, ca_k$ >, <*T*>, <*S*>, < $op_1, op_2, \ldots, op_s$ >} and *att''* = {<$sa'_1, sa'_2, \ldots, sa'_m$>, < $oa'_1, oa'_2, \ldots, oa'_n$ >, < $ca'_1, ca'_2, \ldots, ca'_k$ >, <*T*>, <*S*>, < $op'_1, op'_2, \ldots, op'_s$ >}. The binary operation f_i (*att*, *att'*) is equivalent to performing the binary operation on each attribute value item in *att*, i.e., f_i *(sa, sa')*, and similarly for other attributes. The result of f_i *(att, att')* is still an attribute authorization item. Therefore, (*ATT*, *FA*) forms an algebraic system. □

3.4. Policy Composition Algebra

With the basic concepts above, we can now put forward the formal definition of policy composition. For any policies pol_1 and pol_2, along with an access request in the form of an attribute authorization item *att*, we have:

Definition 1. ***Negation Operator (¬)*** *¬ pol_1 represents a new access control policy that states if att is evaluated as deny access by pol_1, then it is evaluated as permit by ¬ pol_1. If access authorization is evaluated as not applicable, then it is evaluated as conflict.*

Definition 2. ***Union Operator (∨)*** *$pol_1 \vee pol_2$ represents a new access control policy that states if att is permitted by pol_1 and not denied by pol_2, or permitted by pol_2 and not denied by pol_1, then it is permitted by $pol_1 \vee pol_2$. Intuitively, this operator combines the attribute authorization items of pol_1 and pol_2.*

Definition 3. ***Intersection Operator (∧)*** *$pol_1 \wedge pol_2$ represents a new access control policy that states if att is permitted by both pol_1 and pol_2, then it is permitted. Intuitively, this operator extracts the common attribute authorization items.*

Definition 4. ***Subtraction Operator (-)*** *pol_1-pol_2 represents a new access control policy that states if att is permitted by pol_1 and not permitted by pol_2, then it is permitted in pol_1-pol_2. This means that the access request of the subject needs to subtract the overlapping attribute authorizations from pol_1. Intuitively, it removes the attribute authorization items of pol_2 from pol_1. Clearly, this operator can be used to define negation of authorization.*

Definition 5. ***Permit-overrides Operator ($\underline{\vee}$)*** *$pol_1 \underline{\vee} pol_2$ represents a new access control policy that if att is evaluated as permit by pol_1 and also evaluated as permit by pol_2, or evaluated as permit by pol_1 and evaluated as not applicable by pol_2, then the access is permitted by the new synthesized policy.*

Definition 6. ***Deny-overrides Operator ($\overline{\wedge}$)*** *$pol_1 \overline{\wedge} pol_1$ represents a new access control policy that if att is permitted by pol_1 and also evaluated as permit by pol_2, the access is permitted by the new synthesized policy. If att is evaluated as deny access by pol_1 or evaluated as deny access by pol_2 without a result of permit, then the att is evaluated as deny by the new synthesized policy. If att is evaluated as not applicable by pol_1 and also evaluated as not applicable by pol_2, then the access authorization is evaluated as not applicable by the new synthesized policy.*

Definition 7. ***Constraint Operator (^con)*** *pol_1^con means that the new synthesized policy needs to satisfy both the policy pol_1 and the constraint condition con, where con can be a predicate expression determined through negotiation by the participants involved. Intuitively, the ^con operator adds a constraint condition con to pol_1, removes attribute authorization items that do not satisfy con, and narrows down the scope of pol_1. The ^con operator can be seen as a higher-order operator with the parameter con, and it depends on the specific constraint con, which is generally composed of predicates or relational expressions. In this case, we select binary logic to limit the evaluation of constraint condition con.*

Definition 8. ***Function Operator (f_w)***. *f_w (pol_1, pol_2) refers to a new policy obtained by synthesizing the access control policies pol_1 and pol_2 through certain operations based on common mathematical formulas or user-defined operators. f_w is a series of operator binary operator on attribute tuples, and it can also be seen as a flexible higher-order operator with the parameter w, which depends on the operator w of the algebraic system (ATT, FA). It can be understood that w is actually the combined effect of binary operator extensions on different attribute value domains.*

We have introduced some unary and binary policy operators, and their synthetic matrixes are shown in Figure 4. However, they cannot deal with situations that consider the combination of sub-policies as a whole, rather than through a step-by-step process of combining two results. In particular, this approach cannot express counting-based strategies such as weak-majority or strong-majority.

pol_1	1	0	⊥	⊤
$\neg\, pol_1$	0	1	⊤	⊥

(**a**) $\neg\, pol_1$

$pol_1 \setminus pol_2$	1	0	⊥	⊤
1	1	⊥	1	1
0	⊥	0	0	0
⊥	1	0	⊥	⊥
⊤	1	0	⊥	⊤

(**b**) $pol_1 \vee pol_2$

$pol_1 \setminus pol_2$	1	0	⊥	⊤
1	1	⊤	⊤	⊤
0	⊤	0	⊤	⊤
⊥	⊤	⊤	⊤	⊤
⊤	⊤	⊤	⊤	⊤

(**c**) $pol_1 \wedge pol_2$

$con \setminus pol_1$	1	0	⊥	⊤
1	1	0	⊥	⊤
0	0	0	0	0

(**g**) $pol_1 \wedge con$

$pol_1 \setminus pol_2$	1	0	⊥	⊤
1	⊤	⊤	1	⊤
0	⊤	⊤	0	⊤
⊥	⊤	⊤	⊥	⊤
⊤	⊤	⊤	⊤	⊤

(**d**) pol_1-pol_2

$pol_1 \setminus pol_2$	1	0	⊥	⊤
1	1	1	1	1
0	1	0	0	0
⊥	1	0	⊥	⊤
⊤	1	0	⊤	⊤

(**e**) $pol_1 \veebar pol_2$

$pol_1 \setminus pol_2$	1	0	⊥	⊤
1	1	⊤	⊤	⊤
0	⊤	0	⊤	⊤
⊥	⊤	⊤	⊤	⊤
⊤	⊤	⊤	⊤	⊤

(**f**) $pol_1 \barwedge pol_1$

Figure 4. Figure of several operators in matrix form.

Definition 9. ***Linear constraint.*** *A linear constraint is an expression that connects a number of linear equations or inequations on variables Ps, Ds, NAs, and CLs using conjunctive operator* $\wedge$ *and disjunctive operator* $\vee$*, where Ps, Ds, NAs, and CLs stand for the number of sub-policies that return permit, deny, not applicable, and conflict, respectively.*

Table 3 shows how to use linear constraints to specify deny-overrides, only-one-applicable, weak-consensus, strong majority [18] and trust-based voting. Trust-based voting is expressed as $V_{m,n}$ (pol_1, pol_2, …, pol_n), where $n \geq 2$, $m \leq n$, m is determined through negotiation by the n participating policies. This means that the access request of a subject must satisfy at least m policies in the synthesized policies, and among these m policies. The voting operator requires that the trust level of the subject is valid within a certain time period with meeting a certain threshold of trust T_{thd}, and the policy from the domain where the object resides must be participating in the process and it should be satisfied. The determination of T_{thd} in the policy synthesis is based on the requirements of the access control policy in the domain where the object resource resides. In other words, the participating parties in the access control policy synthesis first filter out policies with low trust requirements for the subject, to prevent malicious subjects from participating in policy synthesis and avoid privacy information leakage and attacks on the object resource. Then, the first round of filtering is performed for the policy synthesis, removing redundant policies, and improving the efficiency of policy synthesis while ensuring resource security.

Table 3. Using linear constraints to specify policy combination.

POL	Deny-Override	Only-One-Applicable	Weak Consensus	Strong Majority	Trust-Based Voting $V_{m,n}$
1	$Ps > 0 \wedge Ds = 0 \wedge CLs = 0$	$Ps = 1 \wedge Ds = 0 \wedge CLs = 0$	$Ps > 0 \wedge Ds = 0 \wedge CLs = 0$	$Ps > Ds + NAs + CLs$	$Ps \geq m \wedge NAs + CLs \geq Ds \wedge T > T_{thd}$
0	$Ds > 0$	$Ps = 0 \wedge Ds = 1 \wedge CLs = 0$	$Ps = 0 \wedge Ds > 0 \wedge CLs = 0$	$Ds > Ps + NAs + CLs$	$Ps < m \wedge T \geq T_{thd}$
⊤	$Ds = 0 \wedge CLs > 0$	$Ps > 1 \vee Ds > 1 \vee \mathrm{IN} > 0$	$(Ps > 0 \wedge Ds > 0) \vee CLs > 0$	$(Ps \leq Ds + NAs + CLs) \wedge (Ds \leq Ps + NAs + CLs) \wedge (Ps + Ds + CLs > 0)$	$NAs + CLs \leq Ds \wedge T \geq T_{thd}$
⊥	else				

4. Access Control Policy Conflict Detection and Resolution

According to the requirements of Classified Protection of Cybersecurity, different security domains may adopt different access models to ensure the security of data resources.

For example, the railway ticket network and the train dispatching and commanding network are four-level systems, so they must adopt the rules of mandatory access control to authorize access requests. Therefore, access control requests in multilayer rail transit systems often involve several logical security domains and require the combination of multiple policies to implement. When different access control models interact during cross-domain access, conflicts may arise when the authorization results of the subjects are inconsistent. The more models involved in the interaction, the higher likelihood of policy conflicts. Therefore, a model compatible form of TSABAC with common models is put forward, based on which an access control conflict detection and resolution are realized with a combination of multiple priority principles.

4.1. Compatible Policy of TSABAC

Due to the complexity of the multilayer rail transit system, different access control models may be used in different security domains. To get a universal expression of different access policy models, the TSABAC model can be expanded into a compatible TSABAC form. We specify the different policy characteristics as the condition attributes, that is $CA = \{modifier, ea, Ts, State\}$. As such, the compatible policy can be expressed as:

$$pol = < sa, oa, ea, T, S, op, modifier, T_s, State, eff > \quad (11)$$

where:

- ***modifier*** exhibits the characteristics of the DAC model. In this case, the permissions possessed by the subject can be divided into *private* and *public* permissions. Public permissions can be passed on, while private permissions cannot.
- ***sa.rank* != Δ** and ***oa.rank* != Δ** represents an MAC model. In this case, the security levels of the subject and object are pre-assigned by administrators, and they are used as identifiers to check whether the information flow in the access control policy is one-way.
- ***sa.role* != Δ** represents an RBAC model. In this case, permissions are transferred through roles. The policy conflict detection in RBAC is mainly based on the flow direction of role permissions.
- ***Ts*** exhibits the characteristics of the TBAC model. $\boldsymbol{Ts = \{t_1, t_2, \ldots, t_n\}}$ represents a set of tasks, and $\boldsymbol{t_i}$ represents a subset of tasks. In this case, the relationships between tasks can be synchronous, mutually exclusive, sequential, or dependent on delegation of authority.
- ***State*** exhibits the characteristics of the UCON model, and it represents a set of states, i.e., $\boldsymbol{State = \{state_1, state_2, \ldots, state_n\}}$. In this case, conflicts are determined by checking the obligations of the access subject.
- ***ea*** shows the characteristics of the ABAC model, where ***ea*** is the attribute set of the environment.
- Other access control models are described using ABAC attributes, which are unified for description.

4.2. Policy Conflict Detection Based on TSABAC

Access control policy conflicts often occur when a subject is granted two conflicting operation permissions at the same time. According to the entities causing conflicts, access control policy conflicts can be divided into several categories [19]. For any compatible policies pol_1 and pol_2, where $pol_1 = (sa_1, oa_1, con_1, op_1, eff_1)$ and $pol_2 = (sa_2, oa_2, con_2, op_2, eff_2)$, there is

A. Model conflict. Model conflict occurs when an access control policy has a constant which is contradictory to the principle of access control model. For example, if pol_1 is regarded as the MAC model but violates the principle of one-way information flow, a conflict occurs.

B. Modality conflict. When the subjects in two access control policies are the same or have an inheritance relationship, and they perform the same operation on the same resource under the same conditions, but obtain opposite authorization results, it is called a modality conflict. It can be formalized as $sa_1 \cap sa_2 \neq \emptyset$ & $oa_1 = sa_2$ & $con_1 = con_2$ & $eff_1 \neq eff_2$.

C. Condition conflict. When the same or inherited subjects perform the same operation on the same resource, but with different access conditions, resulting in the same authorization result, it is called a condition conflict. It can be formalized as $sa_1 \cap sa_2 \neq \emptyset$ & $oa_1 = sa_2$ & $con_1 \neq con_2$ & $eff_1 = eff_2$.

Different detection methods are applied for different conflict types.

For model conflict, if the attributes item of pol_1 satisfies both *sa.rank* != null & *oa.rank* != null, and *op*1 = "*read*" $\wedge$ *eff* = "1" $\wedge$ *sa.rank* > *oa.rank* $\wedge$ pol_1 is the conflicted policy.

For modality conflict, the detection algorithm is shown in Algorithm 1.

Algorithm 1. Detecting modality conflict

Input: Access policy set *Po*

Output: Access policy set with modality conflict *Pm*, access policy set passing the detection *Po*

```
1: begin
2:     for ∀ pi ∈ Po do
3:         for ∀ pj ∈ pi& i ≠ j do
4:             read each attribute value of pi and pj
5:             if same attribute values exist then
6:                 compare the next attribute value
7:             else if the different value is eff then
8:                 added pi to Pm, and remove pi from Po
9:             end for
10:    end for
11: end
```

For condition conflict, the detection algorithm is shown in Algorithm 2.

Algorithm 2. Detecting condition conflict

Input: Access policy set *Po*

Output: Access policy set with condition conflict *Pc*, access policy set passing the detection *Po*

```
1: begin
2:     for ∀ pi ∈ Po do
3:         for ∀ pj ∈ pi& i ≠ j do
4:             read each attribute value of pi and pj in AA = {SA, OA}
5:             if pi. AA ⊂ pj. AA | pi. AA ⊃ pj. AA then
6:                 read each attribute value of pi and pj in CON
7:                 if pi. CA ⋂ pj. CA ≠ ϕ & pi.eff ≠ pj.eff then
8:                     added pi to Pm, and remove pi from Po
9:         end for
10:    end for
11: end
```

4.3. Policy Conflict Resolution Based on Joint Priority Principles

In the case of conflicts arising from multiple access control policies of different access control models, it is important to resolve them promptly with appropriate priority rules. Focusing on the security requirements of the DAC, MAC, RBAC, TBAC, ABAC, and UCON models, this paper proposes a conflict resolution method based on joint priority principles to solve the problem under the combined effect of multiple access control models. According to characteristics of access control models, they each have a key feature to emphasize in conflict resolution. For example, it is the latest editing time of the policy, the security of the object resource, the access requirements of the access subject role, the subject's task completion time, the trust and sensitivity which are used to monitor the entity behavior, and the authorization during usage for DAC, MAC, RBAC, TBAC, ABAC, and UCON models, respectively.

The process of conflict resolution is shown in Figure 5. First, we add owner attribute and loading time attribute to the policies during preprocessing, where the owner represents the policy-maker, and the loading time specifies the latest time the policy was modified.

Then, the attributes of the owner, specialness, and model are compared, so as to select the policy of obvious higher priority regardless of the content. Moreover, as for the policies of the same model, we choose the corresponding priority principle according to the characteristics of the model itself and perform deep synthesis when required based on the method proposed in Section 3. Finally, consistency judgment is conducted, to determine whether the newly synthesized policy meets the expectations of the entities involved in the policy synthesis. If not, the administrator has the right to specify the result to complete the conflict resolution.

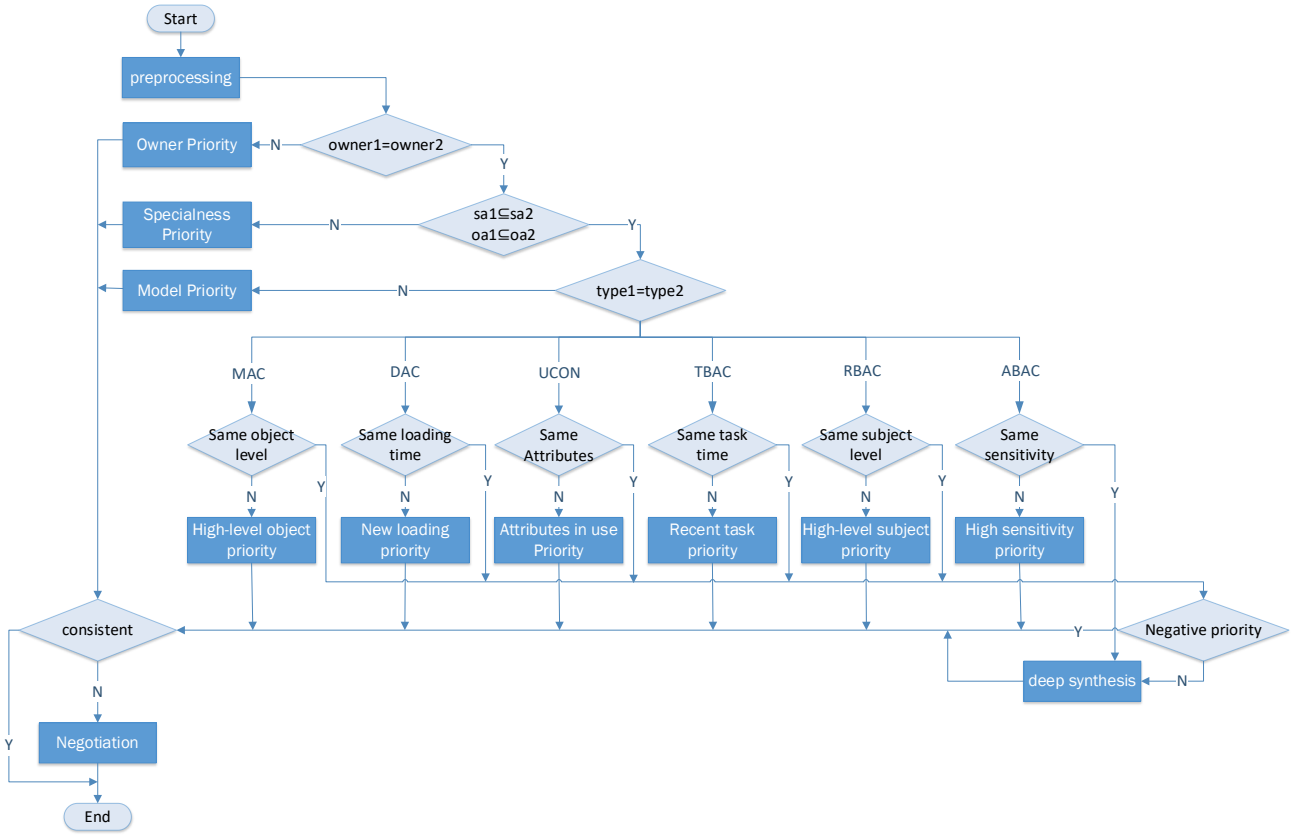


Figure 5. Policy conflict resolution method based on joint priority principles.

The joint priority principles of the conflict resolution are defined as follows:

- **Owner Priority Principle**. If the priorities of the policy owners are not equal, select the policy with the higher priority of the policy owner as the result.
- **Specialness Priority Principle**. A special policy refers to a policy whose subject domain and object domain are included in another one. The special policy is considered to be the resolution result of conflict resolution.
- **Model Priority Principle**. Within multiple access control models, we first determine the type of access control policy based on the Equation (11). If two access control policies conform to different models, the conflict resolution of access control policy is completed according to the predetermined priority order of {MAC, DAC, UCON, TBAC, RBAC, ABAC}.

$$Type\ (pol) = \begin{cases} sap.rank! = null\ \&\ \&oap.rank! = null\ MAC \\ modifier = public\ \|\ modifier = private\ DAC \\ sap.role! = null\ RBAC \\ TA! = null\ TBAC \\ STATE! = null\ UCON \\ else\ ABAC \end{cases} \tag{12}$$

- **High-level object priority principle**. In the MAC model, it focuses on protecting the security of resources. The policy with a higher security level for the object is given priority in conflict resolution.
- **New loading priority principle**. In the DAC model, to ensure the timeliness of authorization, select the most recently loaded access control policy as the result of conflict resolution.
- **Attributes in use priority principle.** In the UCON model, subject attributes change during the access process affect the subject's authorization. Thus, the policy with higher priority for attributes in use is accepted.
- **Recent task priority principle.** In the TBAC model, the most prominent feature is that a task consists of multiple subtasks, and completing the task is given priority. Among them, the subtask with the latest time is given priority.
- **High-level subject priority principle.** In the RBAC model, access control policies focus on the permissions obtained by the subject role, so the role of the subject has higher priority, the subject has higher priority. When the subject priority levels of the two access control policies are inconsistent, the policy with the higher priority level is given priority.
- **High sensitivity priority principle.** In the ABAC model, it focuses on protecting the object resources, so the policy with a higher priority for the object sensitivity has higher priority.
- **Negation priority principle**. When the authorization results of the two policies are opposite, to protect the security of the object resources, denying authorization is given priority.

5. Application and Analysis

In this section, we give an application case of the access control framework of a multilayer domain rail transit system, and analyze the performance of policy resolution, to verify the effectiveness of the framework proposed in this paper.

5.1. Application of Cccess Control Architecture in Multilayer Rail Transit Systems

In multilayer rail transit system, there are generally four security domains, namely the trunk railway, urban railway, intercity railway, and urban metro. This article assumes that each security domain is based on its own access control policy model according to the security requirements. It then uses a unified set of attributes to describe policies and performs policy composition with user-defined operators to accomplish secure cross-domain access. The access control policies for each of these systems are as follows: trunk railway—*Pt*, suburban railway—*Ps*, intercity railway—*Pi*, and urban rail transit—*Pu*. Cross-domain access is achieved through policy composition between logical security domains. By synthesizing policies from different security domains, information resources can be shared across domains with uniform access control management.

Assuming a scenario where a hub station aims to achieve seamless passenger transfers between trunk railway and urban rail transit. They need to share passenger information and provide passenger guidance within the station.

First, let us take a look at the access control architecture for data sharing in multi-domain transportation systems at a macro level [20], as shown in Figure 6. In an urban rail transit system, production management system (PMS) and production auxiliary systems (PAS) are related to the passenger transport as the first-level subclass of business, and the overall policy is represented as $P_{UR} = P_{PMS} \vee P_{PAS}$. PAS has two s-level subclass information systems, i.e., auto fare collection (AFC) system and passenger information system (PIS). AFC provides passenger travel information, including the passenger's on-board and offboard time, travel distance, fare, and other relevant information. The PIS system utilizes these data to calculate estimated arrival times, train operation status, which can be displayed to passengers through displays at stations and inside train cabins, on-board broadcasting, mobile applications, and websites. The ticketing internet platform

(TIP) uses these data to update ticket availability, prices, and seat selection information for users to purchase tickets online. Therefore, the policy of PAS and PMS are expressed as $P_{PAS} = P_{AFC} \vee P_{PIS}$, $P_{PMS} = P_{TIP}$.

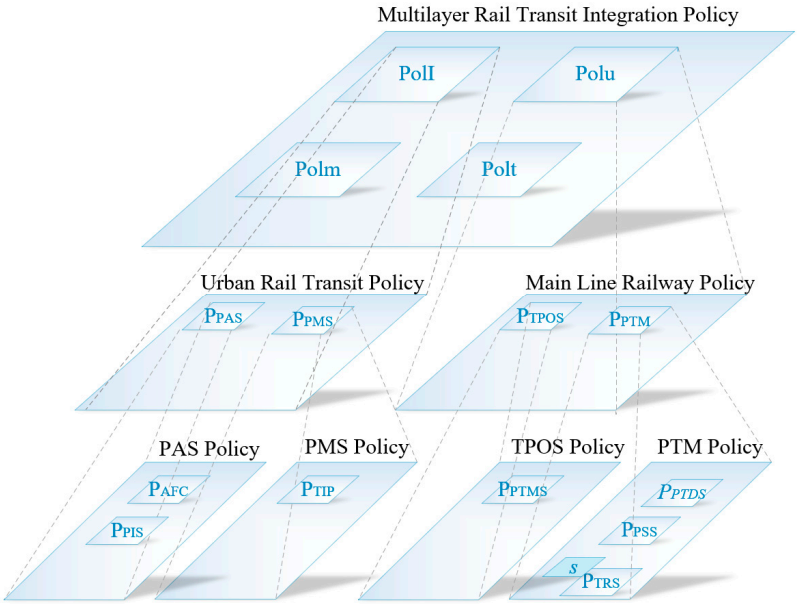


Figure 6. A policy regulating access to multilayer rail transit systems.

While in trunk railway, the information systems associated with passenger transport are the ticket reservation system (TRS), passenger transport marketing decision-support system (PTDS), passenger service systems (PSS), and passenger transport management system (PTMS). The first three of these belong to the business subclass of passenger transport marketing (PTM), and the last one is part of transportation production organization (TPO). Since TRS has a higher hierarchy, the three parts of PTM have different hierarchical definitions, we assume that access to any TRS resource is forbidden to users blacklisted for infraction of rules (e.g., honor code). Therefore, we can write $P_{PTM} = P_{PTDS} \vee P_{PSS} \vee P_{TRS}\hat{}[blacklisted(s)]$ and $P_{TR} = P_{PTM} \vee P_{TPO}$.

5.2. Access Control Policy Composition in Multilayer Rail Transit System

After illustrating the application of the access control framework, we will discuss the specific operations involved in policy composition. For the four security domains, trunk railway, intercity railway, suburban railway, and urban rail transit, we assume their contents of *Pt*, *Pi*, *Ps*, and *Pu* to be shown in Table 4.

Table 4. Contents of *Pt*, *Pi*, *Ps*, and *Pu*.

Pol	SA	OA	CA	T	S	OP
Pt	*sub.level* > 5	*obj.level* ≤ 2 *obj.quality* ≤ 0.7	*link* = secure *date* < 2022.12.30	T > 0.8	S < 3	op = read
Pi	*sub.level* > 5	*obj.level* ≤ 2 *obj.quality* ≤ 0.8	*link* = secure *date* < 2022.12.30	T > 0.8	S < 2	op = read
Ps	*sub.level* > 5	*obj.level* ≤ 2	*link* = secure *date* < 2022.12.31	T > 0.8	S < 3	op = read
Pu	*sub.level* > 5 *sub.quality* ≥ 3	*obj.level* ≤ 3 *obj.quality* ≤ 0.8	*date* < 2022.12.31	T > 0.8	S < 3	op = read

Results of policy composition for the four security domains are analyzed as follows:

A. The results of policy composition between trunk rail and intercity railway

Considering that *Pt* and *Pi* are compatible policies, the possible composition results of policies *Pt* and *Pi* are as follows:

(1) If trunk railway agrees that "access not allowed by intercity railway should not be accessed", the composition result is $pt \wedge pi = pi$.
(2) If intercity railway agrees with "access allowed by trunk railway should be accessed ", the composition result is $pt \vee pi = pt$.
(3) If both trunk railway and intercity railway take a step back, the composition result could be realized by *fw* (*Pt*, *Pi*), where *fw* is the mean operator, and is expressed as:

$$f\omega(Pt, Pi) = \left\{ \begin{array}{l} sa_1.level > 5 >, obj.level \leq 2,\ obj.quality \leq 0.75, \\ link = secure,\ date < 2022.12.30, T > 0.8, S < 2.5,\ op = read \end{array} \right\}$$

Assuming a subject *Q* in a trunk railway system, whose current trust level is 0.9 with a secure level exceeding 5, requests to read the target resource in intercity railway with a security level of 2 and a sensitivity level of 2.3. The current link state is secure, and the access time is 15 December 2022. The attribute authorization item is ATT_Q = {<5>, <2, 0.7>, <secure, 2022.12.15>, <0.9>, <2.3>, <read>}. According to Table 4, $ATT_Q \in f\omega(Pt, Pi)$ satisfies the policy composition result, so *Q* is authorized to read the target resource in this case.

Since the trust level of the subject and sensitivity of the object are dynamically updated, when the access subject interacts with the resource target, if the received feedback indicates a decrease in trust level, it implies that the access subject was deceptive during the previous interaction, leading to restricted authority. Since a decrease in trust level may indicate a malicious node, the currently granted permission should be revoked and reauthorized to protect the security of the resource target. As for the sensitivity, if the object is confronted with growth in visits, the sensitivity may increase and access authorization for this object should be more careful.

The policy composition result between trunk railway and intercity railway demonstrates that the union and intersection operators can perform traditional set operations, and the average value function can be implemented using modal operators. This allows modal operators to handle more complex policy composition scenarios. What is more, the trust and sensitivity attribute can be used to periodically monitor the behavior of access control subjects, preventing illegal activities and ensuring the security of resource targets.

B. The policy composition result between trunk railway and suburban railway.

Note that the policies *Pt* and *Ps* are incompatible due to the fact that *Ps* does not consider the data quality attribute. The compatible results are as follows:

(1) If trunk railway agrees that "access allowed by suburban railway is permitted", the composition result is $Pt \vee Ps \hat{}^{obj.quality>0.7} = Ps$.
(2) If suburban railway agrees that "access not allowed by trunk railway should not be accessed". the composition result is $Pt \wedge Ps \hat{}^{obj.quality \leq 0.7} = Pt$

It demonstrates that ^con operators can transform incompatible policies during policy composition and support constraint operators [8]. In TSABAC, the trust level attribute of the access subject and sensitivity of the target object are both crucial. They reflect the subject's credibility and help protect the security of the resource target. The current trust and sensitivity value participates in the calculation of the next authorization request, serving as the basis for the next authorization.

C. The policy composition result between trunk railway and urban rail transit

Note that the policies *Pt* and *Pu* are incompatible, due to the fact that *Pu* does not consider the subject quality attribute. The compatible results are achieved by negotiation as follows.

Based on the policy merging principles agreed upon by trunk railway and urban rail transit, which include trunk railway agreeing with urban rail transit in terms of subjects

and effective dates, avoiding the leakage of high-security-level information in terms of object security levels and link security, and taking the average value in terms of data quality attribute, the merged result can be obtained as follows:

$$f\omega(Pt, Pu) = \begin{Bmatrix} sub.level > 5, sub.quality \geq 3,\ obj.level \leq 2,\ obj.quality \leq 0.75, \\ link = secure,\ date < 2022.12.31, T > 0.8, S < 3,\ op = read \end{Bmatrix}$$

D. The policy composition result among trunk railway, intercity railway, suburban railway, and urban rail transit

In the first scenario, the common part of the access control policies of trunk railway, intercity railway, suburban railway, and urban rail transit is taken, which requires that the attribute authorization items must be satisfied simultaneously to grant the corresponding access permissions to the authorized subjects. The composited policy is:

$$Pt \wedge Pi \wedge Ps \wedge Pu = \begin{Bmatrix} sub.level > 5,\ sub.quality \geq 3,\ obj.level \leq 2,\ obj.quality \leq 0.7, \\ link = secure,\ date < 2022.12.30, T > 0.8, S < 2,\ op = read \end{Bmatrix}$$

In the second scenario, we assume $TV_{(3,4)}$ (Pt, Pi, Pm, Pu), where the trunk railway is where the resource is located, so the policy composition must include Pt. Therefore, the policy composition is:

$$TV_{(2,3)}(Pi, Ps, Pu) \wedge Pt = \begin{Bmatrix} sub.level > 5,\ sub.quality \geq 3,\ obj.level \leq 2,\ obj.quality \leq 0.7, \\ link = secure,\ date < 2022.12.30, T > 0.8, S < 3,\ op = read \end{Bmatrix}$$

It should be noted that although the composition algebra provides operators to describe the combination of policies, the choice of operators depends on the specific application scenario. The selection of composition operator involves multi-party security policy constraints, which is related to specific application scenarios. As described in this section, the choice of synthesis operator is not the same among organizations. For example, in scenario A, trunk railway chooses the $\wedge$ operator in case (1) and chooses the $\vee$ operator in case (2); in scenario B, urban rail transit may choose different synthesis operators. Since the parties may choose different synthesis operators, different synthesis results may be obtained. Therefore, the evaluation of the synthesis results of each party is helpful to the selection of the final synthesis operator. The quality of the composite result is generally evaluated according to the negotiation result (i.e., the common protection requirements for the aggregated resources agreed by all parties).

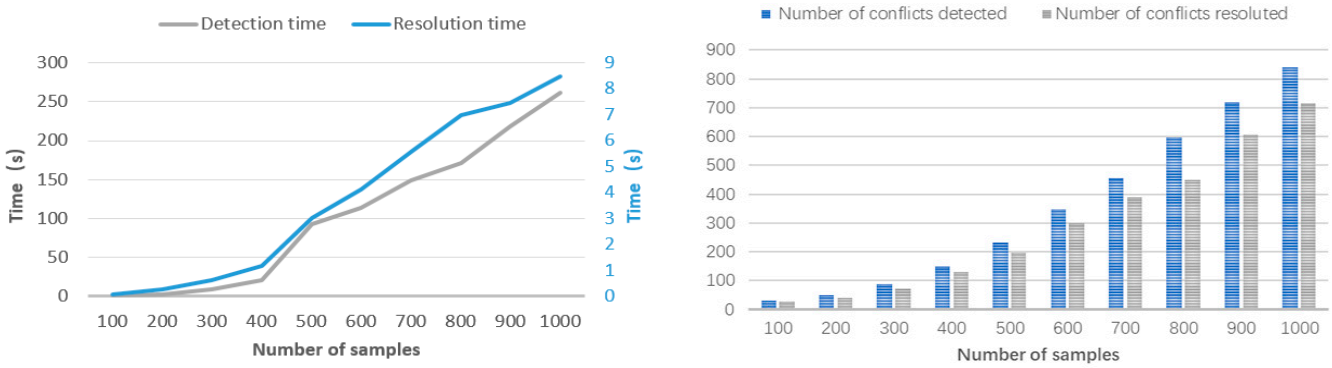
5.3. Performance Analysis of Access Control Policy Conflict Resolution

In the process of access control policy synthesis, the more attributes and authorization items there are in the access control policies, the more complex the synthesis becomes, and the higher the probability of conflicts arising. Therefore, it is common to analyze the synthesis under a fixed number of attributes. When the number of attributes is the same, it indicates that the complexity of the access control policies is similar. Under this condition, the number of conflicts in access control policies will increase with the increase in the number of policies. In other words, the number of conflicts is directly proportional to the number of access control policies. The most important aspect of access control policy synthesis is resolving conflicts through policy synthesis operators and priority principles.

Here, we assume the number of policies involved in access control policy synthesis ranges from 100 to 1000. According to the principles of access control policy resolution, conflicts in access control policies are primarily resolved through the owner attributes of the policies, specific policy priorities, and model priority principles. Ultimately, the synthesis

of the participating access control policies becomes the resolution within the same access control model.

As for the time performance shown in Figure 7a, during the process of resolving access control policy conflicts, access control policies based on trust attributes can first filter the policy set for the accessed resources based on the trust level and the sensitivity. This filtering reduces the number of policies involved and improves the efficiency of conflict detection. However, in the process of synthesizing access control policies, the impact of changing attributes on conflict resolution should be considered. The worst case is when the trust level of the subject suddenly decreases after conflict resolution, requiring the re-synthesis of access control policies to protect the security of resources. The best case is when the trust level attribute of the subject last updated before access control policy synthesis, and remains unchanged throughout the access process, reducing the number of policy synthesis instances. Although the worst case requires more time, it ensures the security of resources and improves the overall security of the system, making the expenditure of time worthwhile. Since the computation and update time for trust level values is short, it can be ignored.



(**a**) Time performance (**b**) Accuracy performance

Figure 7. The performance of policy conflict detection and resolution with 10 groups of data with the step size of 100 sample.

As for the accuracy performance shown in Figure 7b, previous research has shown that the optimal conflict resolution rate for various models is generally around 80% [21], while the resolution based on joint priority principles has a significant increase to 85%. In addition, before applying the optimal algorithm for access control policy synthesis in each model, the number of access control policies should be reduced to at least one-third of the original number, when the number of access control policies is reduced within the same model through owner priority and specific policy priority. Therefore, it can be concluded that the conflict resolution algorithm based on joint priority principles has already reduced the number of policies involved in access control policy synthesis during the initial screening phase. Therefore, the conflict resolution algorithm based on joint priority principles proposed in this paper for access control policy synthesis is more efficient and secure.

6. Conclusions and Future Work

This paper focused on the access control framework between different systems, aiming to break down the data silos and create data interaction during the construction and operation multilayer rail transit system. According to the challenging demand of security and granularity, the TSABAC model is put forward to describe the characteristics of the access control process based on the universal categorization and hierarchization of data resources. Furthermore, the method of policy integration is discussed, as well as the solution of the policy incompatibility problem, due to cross-domain interaction. Compared with related

work, the results in Table 5 show that the framework was fine-grained, particularly secure, functionally complete, and highly compatible. Future work should improve the efficiency of conflict detection and resolution algorithms, to achieve better time performance.

Table 5. Comparisons of TSABAC-based mechanism in this paper with related work.

	Fine-Grained Control	Universal Security Measures	Policy Combination	Policy Conflict Detection	Policy Conflict Resolution
MAC-based [5]		✓	✓		
Zero-trust MAC-based [6]	✓	✓	✓		
RBAC based [7]	✓		✓		
Block-chain-based [8]		✓		✓	✓
Real-time credibility-based [9]	✓	✓	✓		
TSABAC based	✓	✓	✓	✓	✓

Author Contributions: Conceptualization, Z.M., Y.W. and X.G.; methodology, X.G. and Y.L.; validation, X.G.; investigation and supervision, Z.M. and Y.W.; writing—original draft preparation, X.G.; writing—review and editing, X.G. and Y.L. All authors have read and agreed to the published version of the manuscript.

Funding: The work was supported by Fundamental Research Funds for the Central Universities (No. 2022JBCZ005) and Important Projects of China Railway (No. N2023S002).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data presented in this study are available on request from the corresponding author. The data are not publicly available due to privacy.

Acknowledgments: The authors wish to thank the reviewers for their valuable comments and suggestions concerning this manuscript.

Conflicts of Interest: Author Xin Geng and Yu Liu are employed by the China Railway Information Technology Group Co., Ltd. Author Zhisong Mo is employed by the China State Railway Group Co., Ltd. The remaining authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

References

1. Pan, Z.; Zhang, T.; Tang, H.; Wang, Y. Research on the "Four-Network Integration" System of Multi-Level Rail Transit. *Transp. Eng.* **2020**, *20*, 1–8.
2. Yu, X.; Zhang, L. Research on the four networks integration development of Beijing rail transit and railway. *Mod. Urban Rail Transit* **2021**, *1*, 1–6.
3. Liu, Y.; Li, L.; Lu, F.; Wang, C.; Wang, L. Key technologies of data governance of "four-network integration" for rail transit. *Railw. Comput. Appl.* **2023**, *32*, 82–86.
4. Li, Q. Railway Data Security Governance System and Privacy Computing Technology Research. Ph.D. Thesis, China Academy of Railway Sciences, Beijing, China, 2023.
5. Zhu, L. Research and Implementation of the Mandatory Access Control on Gateway Devices in Railway Information System. Ph.D. Thesis, Beijing Jiaotong University, Beijing, China, 2014.
6. Suo, X.; Qi, S.; Zhang, Y.; Zhu, H. Research on fine-grained access control scheme of railway cloud platform. *Railw. Comput. Appl.* **2021**, *30*.
7. Wang, B. Research on Collaborative Design Application of Subway Comprehensive Pipelines Based on RBAC And Bim. Ph.D. Thesis, Xi'an University of Technology, Xi'an, China, 2018.
8. Wu, J. Research on Key Technologies of Railway Data Assets Sharing Based on Blockchain. Ph.D. Thesis, China Academy of Railway Sciences, Beijing, China, 2022.
9. Yu, W.; Zhang, L.; Xu, Q. Real-Time Reliability Access Control Based on Rail Traffic Data Platform. *Electronics* **2023**, *12*, 1105. [CrossRef]

10. Zhang, L. Cloud Computing Based Railway Information Sharing Platform and Key Technologies Research. Ph.D. Thesis, China Academy of Railway Sciences, Beijing China, 2013.
11. *GB/T 37988-2019*; Information Security Technology—Data Security Capability Maturity Model. State Administration for Market Regulation: Beijing, China, 2019.
12. Wang, J. Study on Technology of Access Control of Attribute-Based Encryption and Emergency Decision of Shared Data of High-Speed Railway. Ph.D. Thesis, Beijing Jiaotong University, Beijing, China, 2017.
13. Zhou, L.; Zhang, X.; Qiu, Y.; Zhu, Y.; Miao, S.; Jiang, L. Research on Power Data Classification and Grading Method. *Electr. Power Inf. Commun. Technol.* **2023**, *21*, 25–30.
14. Han, D.-J.; Gao, J.; Zhai, H.-L.; Li, L. Research Development of Access Control Model. *Comput. Sci.* **2010**, *137*, 29–33+43.
15. Xing, Y.; Wang, X.; Han, X.; Zhang, C. Influence of network nodes in new media environment based on information entropy—A case study of WeChat public account. *Libr. Inf. Work* **2018**, *62*, 76–86.
16. Wang, J.; Luan, J.; Tan, Y. Research on big data access control model based on data sensitivity. *Comput. Eng. Appl.* **2019**, *55*, 70–77.
17. Zhao, P.; Wu, L.; Hong, Z.; Sun, H. Research on multicloud access control policy integration framework. *China Commun.* **2019**, *16*, 222–234. [CrossRef]
18. Li, N.; Wang, Q.; Qardaji, W.; Bertino, E.; Rao, P.; Lobo, J.; Lin, D. Access control policy combining: Theory meets practice. In Proceedings of the 14th ACM Symposium on Access Control Models and Technologies (SACMAT '09), Stresa, Italy, 3–5 June 2009; Association for Computing Machinery: New York, NY, USA, 2009; pp. 135–144.
19. Ma, X.-P.; Li, Z.-Y.; Lu, J.-F. Research on Specification Language and Policy Conflict of Access Control Policy. *Comput. Eng. Sci.* **2012**, *34*, 48–52.
20. Bonatti, P.; De Capitani di Vimercati, S.; Samarati, P. An algebra for composing access control policies. *ACM Trans. Inf. Syst. Secur.* **2002**, *5*, 1–35. [CrossRef]
21. Hu, J. A Privavy-Awaer Access Control Police Composition Research in Cloud Computing Environment. Ph.D. Thesis, Beijing University of Technology, Beijing, China, 2016.