electronics

MDPI

Article

Real-Time Reliability Access Control Based on Rail Traffic Data Platform

Wenjuan Yu, Lei Zhang * and Qian Xu

Department of Traffic Information and Control Engineering, Tongji University, Shanghai 200092, China
* Correspondence: reizhg@tongji.edu.cn

Abstract: With the introduction of the industrial internet, Internet of Things, and big data technology, the interconnection degree of the industrial control cloud network is getting higher and higher, the data interface needs to be gradually standardized, and there are more and more open interface components. Data-based attacks will continue to emerge. The real-time and reliability of access control are essential for trust value updating between network participants. This paper proposes a fine-grained dynamic real-time credibility access control method based on zero trust. Continuous authentication and trust evaluation should be carried out throughout the access control process. The zero-trust evaluation indicators of a rail transit data platform that conforms to the requirements of grade protection 2.0 are established. According to the risk feedback, the current trust level is dynamically updated in real time, and the results are used in the access control model. It can reject unauthorized access, reduce the occurrence of illegal intrusion data leakage and data loss events, and has great value in rail transit data security.

Keywords: zero trust; dynamic authorization; access control; data platform

1. Introduction

With the gradual application of emerging technologies, such as cloud computing and big data, in the urban rail transit industry, automation, informatization, and intelligence have become the inevitable trend of urban rail transit development. There are a large number of external service systems in the rail transit industrial control cloud system management network [1]. Due to the network boundary layers of defense, strong attack methods have a higher cost on the network. Attackers often use methods such as phishing software to infiltrate the network to carry out attacks [2]. This can bypass the safeguards of network border security. In addition, for high-risk business and data, system internal staff and outsourced personnel usually have legitimate access rights. There are also serious consequences if there are problems such as loss of credentials, abuse of permissions, or malicious unauthorized access. Therefore, the rail transit industrial control cloud system needs a more secure scheme than the traditional border protection mode to ensure that it can resist APT attacks that bypass traditional detection methods and defense technologies.

Zero trust is suitable as the core idea of information security protection in the industrial internet [3]. Technologies such as comprehensive depth perception, real-time transmission and exchange, fast computational processing, and the advanced modeling analysis of industrial data, have been widely used. The deployment of 'zero trust' architecture enables intelligent control, operation, and organizational optimization of the entire ecological chain. It has great value in data security, which can deny unauthorized access and reduce the occurrence of illegal intrusion, data leakage, and data loss events.

At present, the mainstream trust models generally have the problems of difficulty in accurately predicting the trust degree, excessive dependence on the trusted third party, and the inability to ensure the security of trust data [4]. This paper adopts the idea of zero trust in the stages when the subject applies to access the object, when the subject

Citation: Yu, W.; Zhang, L.; Xu, Q. Real-Time Reliability Access Control Based on Rail Traffic Data Platform. *Electronics* **2023**, *12*, 1105. https://doi.org/10.3390/electronics12051105

Academic Editor: Antoni Morell

Received: 5 January 2023
Revised: 10 February 2023
Accepted: 21 February 2023
Published: 23 February 2023

accesses the object, and when the subject completes the access to the object [5]. With the subject attribute, object attribute, environment attribute, and trust value, the access request is continuously evaluated, and dynamic access control authorization is performed. According to the principle of zero trust, calculating the trust value of the subject is one of the preconditions for granting access rights. This allows for more fine-grained control over access rights after attribute evaluation. It provides necessary and minimal access to mitigate possible security risks. It is worth mentioning that the concepts of zero trust and trust value here do not conflict. The access control architecture is based on the idea of zero trust 'Do not give default trust to all network participating entities', that is, the current credibility of all network participants should be determined in real time. There are three main contributions in this paper. First, a fine-grained dynamic real-time reliability access control framework based on zero trust is constructed. Second, the dynamic updating method of trust is improved. Third, the zero-trust evaluation factor of a rail transit data platform that meets the requirements of grade protection 2.0 is established.

In the field of the rail transit industrial control system, combined with the use of black- and whitelists and user roles, the most widely used access control technique is the approach based on network boundaries. At present, various cities have gradually adopted cloud schemes to build industrial cloud platforms with unified standard interfaces and data formats, providing a good platform foundation for intelligent application construction. The establishment of a security service operation center transforms the single-line information collection into a unified processing and analysis mode. This provides the basis for the zero-trust dynamic access control model, which collects attribute information extensively and updates the state of trust evaluation constantly.

This paper is organized as follows: Section 2 describes the related work of previous studies. Section 3 presents the real-time trust calculation method. Section 4 introduces the feedback-based dynamic update method of trust. Before concluding in Section 6, Section 5 presents the real-time trustworthiness access control method based on the rail transit data platform.

2. Related Work

2.1. Zero-Trust Access Control

Since the prototype of zero trust, location-based implicit trust, was proposed in 2004, the theoretical framework of zero trust and its key technologies have been highly valued by academia and industry [2]. Six years later, John formally introduced the term 'zero trust' and described the associated model [6]. Zero trust has been used in many important practices in the industry. For example, in 2017, Google completed BeyondCorp [7], a project built on zero trust. In 2020, the Cloud Security Alliance held a Zero Trust conference, emphasizing that zero trust has become a key technology and major trend in network security [8].

Zero trust has been applied in government agencies, finance, transportation, operators, medical treatment, manufacturing, and other fields [9]. The Wenzhou Big Data Development Administration used the SDP technology provided by An Heng Information [10]. Shandong Port Group adopted the SDP technology provided by Sangfor [11]. Sunshine Insurance Group's pension and real estate center uses the SDP technology provided by Cloud with deep interconnection [12]. At present, the understanding of zero-trust architecture in the industry is converging. Based on the architecture given by NIST, access control is divided into policy decision points and policy enforcement points [13]. Core technologies include identity security access, agent access control, and trust evaluation.

The core of zero-trust architecture is access control over resources [14]. The purpose of access control is to restrict the user's behavior and operation. It is a method to explicitly allow or limit the access capability and scope by means of control policies, whitelisting, etc. For each network actor, continuous trust evaluation is a key means to build trust from scratch [15]. Malicious access requests may appear after seemingly secure access requests. Continuous verification is therefore necessary. By building a trust evaluation engine including a trust evaluation model and algorithm, the ability of identity-based

trust evaluation is realized [16]. The trust evaluation engine continuously receives log information, combined with the information of the identity library, permission library, and policy library [17]. Based on the continuous analysis of access behavior, trust is continuously evaluated. In the process of interaction, the trust evaluation results are constantly adjusted to cover the 'in progress' access security. When the access subject, context, and environment are at risk, it is necessary to adjust the access rights in real time [18].

2.2. Trust Model

The trust model conducts the authentication and authorization of the subject in a single access, and the access control policy is dynamically adjusted with the change of the state of the subject [19]. Beth et al. proposed the concept of trust management earlier and applied it in the computer field [20]. This provided valuable ideas for the subsequent research on trust models. Later, it was applied in Google's BeyondCorp and Tencent's zero-trust security solution [21]. In order to better measure the trust degree of individuals in the network, some researchers have applied social relationships to the trust model. Bao et al. classified the social relationship of nodes by a collaborative filtering method, and then selected the trusted recommendation nodes [22]. Abderrahim et al. classified network nodes according to their community interests, and selected different trust calculation methods for different categories of nodes [23].

In 2003, Yager proposed the concept of the induced ordered weighted averaging (IOWA) operator based on the OWA operator. It is a weighted average operator between the maximum and minimum operators, which can be used to effectively fuse multiple sets of fuzzy and uncertain information. In 2010, Li [24] introduced the IOWA operator to construct the new combined direct dynamic trust forecasting model, to make up for the shortcomings of the traditional method, and the model hence can have better rationality and a higher practicability. Xiong [25] introduced the IOWA operator into grid authorization management and adopted authorization feedback, based on a satisfaction evaluation factor, to update the trust value of grid management access control. According to the zero-trust concept, continuous authentication and trust evaluation are required throughout the access control process. Since this model has more robust dynamic adaptability, it is very suitable for the trust evaluation phase of this paper. On this basis, this paper modifies the model to make it conform to the principle of zero trust and improves the computational efficiency and decision-making speed.

3. Access Control Model

3.1. Model Overview

The framework of the access control model according to the previous research work is shown in Figure 1 [26,27]. The access authorization process is divided into three main steps: ① role-based access control (RBAC); ② attribute-based access control (ABAC); and ③ trust-based access control (TBAC).

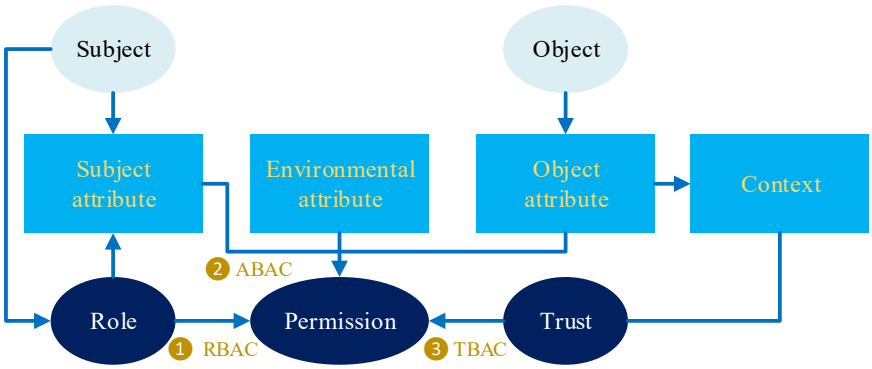

Figure 1. Access control policy.

Step 1: Role evaluation:

Determine the role of the access subjects and preliminarily determine the authorization scope through the corresponding permissions of the roles.

Step 2: Attribute evaluation:

Compare the policy sets through the obtained subject attributes, object attributes, and environment attributes to narrow the scope of authorization.

Step 3: Trust evaluation:

Through the context information, dynamically evaluate the trust value of the access subject, constantly update the current trust value to further narrow the scope of authorization, and finally confirm the authorization permission.

The first step is to adopt the RBAC model, which is a part of static access control [28]. It is the static relationship between access subjects and permissions. In the static part of the model, most elements of the RBAC model in the NIST standard are retained, including subjects, roles, and permissions, while the second and third steps use the ABAC model and TBAC model, which are a part of dynamic access control. The dynamic part of the model uses the obtained attributes to filter permissions, that is, to narrow down the permissions of the subject. The subject attribute (ATT(S)) is defined for the access subject, the object attribute (ATT(O)) is defined for the access object, and the environment attribute (ATT(E)) is defined for the environment. Combined with context information, the trust value of the access subject is dynamically evaluated. According to the feedback, the current trust value is constantly updated, and the authorization permission is finally confirmed.

3.2. Formulation Strategy

3.2.1. Definition

- Subject, S: network agents that initiate access requests, including users, devices, and applications.
- Role set, R: the role to which the subject initiating the access belongs.
- Object set, O: what the network agent requests to access, including user application, interface, function, data, etc.
- Attribute set, ATT: information that identifies the characteristics of access control participants, such as subject and object, including subject attribute ATT(S), object attribute ATT(O), and environment attribute ATT(E).
- Context, C: the external environment in which the subject interacts with the object is a collection of some subject attributes, object attributes, and environmental attributes.
- Trust degree, T: the trust value of the object when the object performs an operation or task on the subject, the representation of the credibility of the behavior, and the dynamic evaluation of the subject's trust degree in the context.
- Permission set, P: the operation permission of the subject to the object it requests to access.

3.2.2. Description

According to the standard definition of the RBAC model, the model involved in this paper is described in the following Table 1.

Table 1. Model definition based on RBAC model.

1. RBAC Sets and Functions.
SUBJS, ROLES, OPS, and OBS (subjects, roles, operations, and objects);
PERMS $\in 2$ ($^{OPS \times OBS}$), the set of permissions;
SESSIONS, the set of sessions;
subject _ sessions (s: SUBJS) $\rightarrow 2^{SESSIONS}$, the mapping of subject s onto a set of sessions;
avail _ session _ roles (s: SUBJS) $\rightarrow 2^{ROLES}$, the mapping of subject s onto a set of roles;
avail _ session _ perms (rs: 2^{ROLES}) $\rightarrow 2^{PERMS}$, the mapping of a set of roles onto a set of permissions;
SA $\subseteq$ SUBJS $\times$ ROLES, a many-to-many mapping subject-to-role assignment;
PA $\subseteq$ ROLES $\times$ PERMS, a many-to-many mapping role-to-permission assignment.

Table 1. *Cont.*

2. Additional Sets and Functions of this Paper.
T represents the values of trust, a finite set of values. ATT(S), ATT(E), ATT(O), and C represent finite sets of subject, environment object, and context attribute functions, respectively. For each att in ATT(S)∪ATT(E)∪ATT(O)∪C, Range(att) represents the attribute's range, a finite set of atomic values. att Type: ATT(S)∪ATT(E)∪ATT(O)∪C→{set, atomic}. Specifies attributes as set- or atomic-valued. Each attribute function maps elements in SUBJS and OBS to atomic or set values. filter _ r(r: ROLES)→$2^{POLICIES\_R}$, the mapping of role onto a set of policies. For each pr∈ POLICIES _ R. pr: SUBJS ×ROLES × $2^{ATT(S)}$ × $2^{ATT(O)}$ × $2^{ATT(E)}$→{T, F}. filter _ *p*(*p*: PERMS)→$2^{POLICIES\_P}$, the mapping of permission onto a set of policies. For each pp∈POLICIES _ P. pp: SUBJS × ROLES × PERMS × $2^{ATT(S)}$ × $2^{ATT(O)}$ × $2^{ATT(E)}$→{T, F}. filter _ t(t: TRUST)→$2^{POLICIES\_T}$, the mapping of trust onto a set of policies. For each pt∈ POLICIES _ T. pt: SUBJS × ROLES × TRUST × PERMS × $2^{ATT(S)}$ × $2^{ATT(O)}$ × $2^{ATT(E)}$→{T, F}.

3.3. Access Control Flow

The common zero-trust architecture includes: access subject, access object, trusted agent, dynamic access control engine, trust evaluation engine, identity security infrastructure, data plane, and control plane. Core technologies include identity security, access agent, access control, and trust evaluation. Before the connection between the subject and the object, identity authentication is needed first. The identity management system provides subject attributes to the policy enforcement point. After the subject submits an access request, the policy enforcement point submits a decision request to the policy decision point. The policy decision point makes a request to the trust assessment to feedback the trust value. After obtaining the feedback, the policy decision point performs trust evaluation and returns the result back to the policy execution point. The policy enforcement point determines the permissions available to the subject. The access control flow is as shown in Figure 2. Among these steps, the process of trust evaluation is carried out continuously.

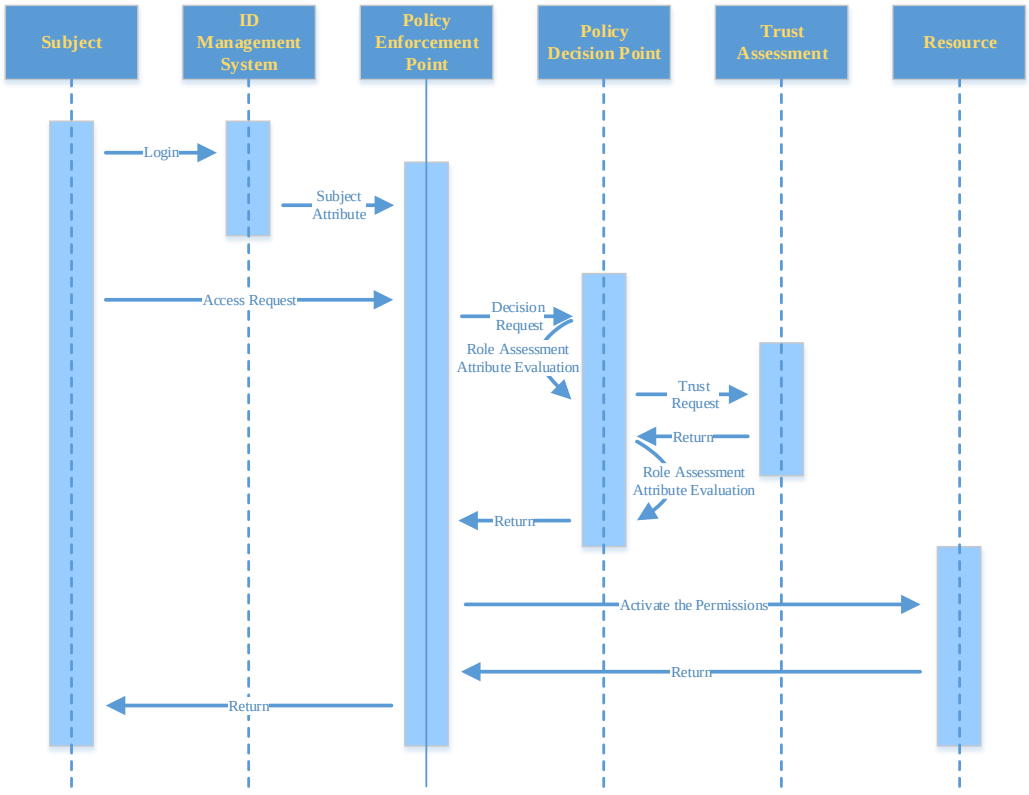

Figure 2. Access Control Flow.

4. Real-Time Trust Calculation

4.1. Trust Calculation Method

As a context-dependent dynamic variable, trust dynamically determines whether to authorize and the scope of authorization [25]. Because of the decisive role of trust in authorization in the zero-trust requirement, the first thing to be solved is trust evaluation. In the process of access control, when the policy decision point receives the decision request submitted by the policy enforcement point, it needs to obtain the trust value of the subject as well as the required attributes for authorization. Moreover, the policy decision point decides whether to allow the subject's access request and the specific access rights according to the authorization policy. In such an authorization mechanism, trust evaluation and authorization are closely related and run through the whole process of the subject (access applicant) accessing the object (data resources). The relationship between trust evaluation and authorization can be described in the following three stages:

- When the subject requests to access the object, in addition to roles and attributes, trust is one of the important bases for the subject to obtain permission. In order to authorize the requester, after the preliminary role evaluation and attribute evaluation, it needs to be evaluated for trust. The historical access behavior of the subject is evaluated, and the trust value is used as the further basis for the authorization decision.
- According to the principle of zero trust, when the subject accesses the object, it should be tacit that there is a risk in the subject's behavior. For real-time fine-grained control, trust evaluation should provide an effective trust update method. The risk of the authorized subject is evaluated, and the trust degree of the interaction is updated through the evaluation results. According to the updated trust degree, the subject's access rights are adjusted to achieve dynamic authorization.
- After the subject accesses the object, it should update the trust value in real time and feedback the risk degree of the process. Through the risk assessment of the behavior of the subject, the overall performance of the subject in terms of multiple zero-trust indicators is obtained, and the trust value of the subject is updated according to the risk assessment value. The updated trust value will be used as the historical trust value of the subject in the next access.

This section describes the first phase of trust calculation. In the traditional access control process, once the access subject passes the identity authentication and static access permission verification, its business access permission is determined. The subsequent abnormal behavior of the access subject is difficult to monitor in real time, and the access permissions cannot be changed in real time. Therefore, the trust dynamic updating algorithm in the second and third stages will be introduced in the next section.

In order to update the access legitimacy of the subject more reasonably, it is set that the behavior of the subject closer to the current interaction time has a greater impact on the current trust evaluation, which meets the requirements of the induced ordered weighted average (IOWA) operator [11]. Therefore, the IOWA operator is used to realize dynamic trust evaluation [24]. In order to characterize the influence and time attenuation of historical trust on trust evaluation, the trust value and its occurrence time after the first n interactions are stored. After sorting the time series of interaction occurrences, the IOWA operator is completely suitable for dynamic trust value evaluation. Historical trust values at different times have different weights in the current trust evaluation, which is shown in Figure 3.

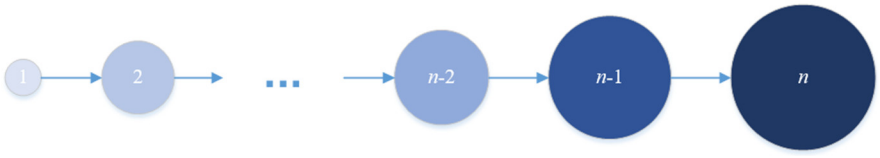

Figure 3. Diagram of trust value passing.

The trust sequence of the nth interaction is

$$S = (T_1(i,j,C), T_2(i,j,C), \ldots, T_n(i,j,C)) \;\; T_t(i,j,C) \in [0,1], 0 \le t \le n \tag{1}$$

Among the variables, n is the number of historical interactions, and $T_t(i,j,C)$ is the trust of data source i to access applicant j under context C of the tth interaction.

The time and trust sequence of the nth interaction:

$$S^{'} = (< t_1, T_1(i,j,C) >, < t_2, T_2(i,j,C), \ldots, < t_n, T_n(i,j,C) >) \tag{2}$$

The current n + 1 trust value is calculated according to the IOWA operator:

$$T_{n+1}(i,j,C) = f_{\mathrm{W}}(< t_1, T_1(i,j,C) >, < t_2, T_2(i,j,C) >, \ldots, < t_n, T_n(i,j,C) >) = \sum_{t=1}^{n} (\omega_t \times a_t(i,j,C))\omega_t \in [0,1] \;, \sum_{t=1}^{n} \omega_t = 1 \tag{3}$$

Among the variables, ω_t is the weight of the historical trust, with the occurrence time ranking at t in the trust evaluation. a_t (i,j,C) is the trust value of t_1,t_2, … ,t_{n}, ranking t from the largest to the smallest.

The maximum entropy method is used to obtain the weighted vector, and the ordered weighted vector of the IOWA operator is the weighted sequence W = (ω_1 ω_2, … , ω_{n}), which meets the conditions maximize : $-\sum_{t=1}^{n} \omega_t \ln(\omega_t)$. The calculation process is shown in Equations (4)–(7).

$$\lambda = \mathrm{Orness}(\mathrm{W}) = \frac{1}{n-1}\sum_{1}^{n}(n-t)\omega_t \tag{4}$$

$$\omega_1[(n-1)\lambda + 1 - n\omega_1]^n = [(n-1)\lambda]^{n-1}[((n-1)\lambda - n)\omega_1 + 1] \tag{5}$$

$$\omega_n = \frac{((n-1)\lambda - n)\omega_1 + 1}{(n-1)\lambda + 1 - n\omega_1} \tag{6}$$

$$\begin{aligned} &\ln \omega_k = \tfrac{k-1}{n-1} \ln \omega_n + \tfrac{n-k}{n-1} \ln \omega_1 \\ &\Rightarrow \omega_k = \sqrt[n-1]{{\omega_1}^{(n-k)} {\omega_n}^{(k-1)}}, k = 2, 3, \ldots n-1 \end{aligned} \tag{7}$$

The value of λ needs to be set according to the requirements. In order to meet the requirement that the longer the current interaction time is, the smaller the impact of the historical behavior on the current trust evaluation is, look for the law of $\mathrm{W} = (\omega_1, \omega_2, \ldots, \omega_n)$ changing with the λ value. Assuming that n is 4, take, respectively, $\lambda = 0, 0.1, 0.2, \ldots, 0.8, 0.9, 1$ and calculate the weight sequence (as shown in Table 2). When λ = 0.5, $\omega_1 = \omega_2 = \omega_3 = \omega_4 = 0.25$. Moreover, the values of $\mathrm{W} = (\omega_1, \omega_2, \ldots, \omega_n)$ are distributed in a centrosymmetric manner.

Table 2. Weights corresponding to different values of λ.

λ \ Weight	ω_1	ω_2	ω_3	ω_4
0	0	0	0	1
0.1	0.0103	0.0433	0.1818	0.7641
0.2	0.0450	0.1065	0.2520	0.5965
0.3	0.0984	0.1647	0.2757	0.4614
0.4	0.1671	0.2133	0.2722	0.3474
0.5	0.2500	0.2500	0.2500	0.2500
0.6	0.3474	0.2722	0.2133	0.1671
0.7	0.4614	0.2757	0.1647	0.0984
0.8	0.5965	0.2520	0.1065	0.0450
0.9	0.7641	0.1818	0.0433	0.0103
1.0	1	0	0	0

Obviously, the longer the interaction time is, the less the impact of historical behavior on the current trust evaluation is. It must be true that $\omega_1 > \omega_2 > \omega_3 > \omega_4$. According to Figure 4, the law of variation is that $W = (\omega_1, \omega_2, \ldots, \omega_n)$ changes with the value of λ. When $\lambda \in (0, 0.5)$, $\omega_1, \omega_2, \omega_3, \omega_4$ gradually increases, not meeting the needs; when $\lambda \in (0.5, 1)$, $\omega_1, \omega_2, \omega_3, \omega_4$ gradually decreases, and is in line with the facts.

Take $\lambda = 0.8$, a group of time trust array sorted by interaction time distance as

$$S^{'} = (< 4, 0.4 >, < 3, 0.9 >, < 2, 0.8 >, < 1, 0.9 >) \tag{8}$$

The permission sequence:

$$W = (0.5965, 0.2520, 0.1065, 0.0450) \tag{9}$$

It can be obtained by simple calculation that the current trust value is

$$T_{n+1}(i, j, C) = 0.5965 \times 0.4 + 0.2520 \times 0.9 + 0.1065 \times 0.8 + 0.0450 \times 0.9 = 0.5911 \tag{10}$$

which is closest to the historical the trust value of 0.4 of the latest interaction and can timely reflect the changes in the trust of the access applicant, meeting the requirements.

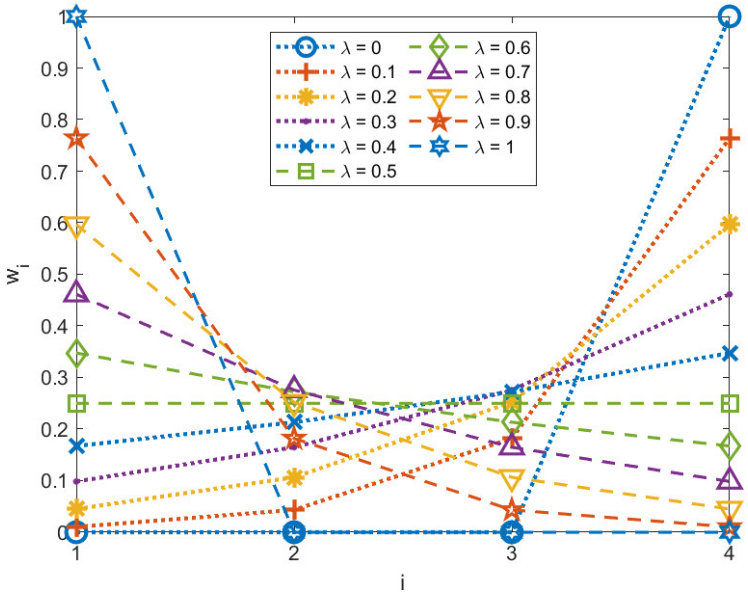

Figure 4. Weights corresponding to different values of λ.

4.2. Trust Rating

The trust level is divided according to the static trust threshold and dynamic trust threshold required for accessing resources. Credibility is divided into five intervals, and each interval corresponds to a trust level. Different trust levels correspond to different access rights. The higher the credibility of the service provider to the service application, the higher the corresponding trust level and access authority of the service application. See Table 3 for the specific classification of trust levels.

Suppose that after the trust policy decision, the permission subset obtained by the service application is P_i' = {read write execute update delete}, where $P_{0'}$ = null, $P_{1'}$ = {read}, $P_{2'}$ = {read, download }, $P_{3'}$ = {read, download, execute}, and $P_{4'}$ = {read, download, execute, update, delete}, and the trust value of the subject can be graded using the determined dividing points, Ψ = {A1, A2, A3, A4} is Ψ = {0.3, 0.6, 0.8, 0.9}; then, the trust policy can be defined as the trust–permission mapping function:

$$f(T,P) = \begin{cases} P_0^{'} & 0 \le T \le 0.3 \\ P_1^{'} & 0.3 \le T \le 0.6 \\ P_2^{'} & 0.6 \le T \le 0.8 \\ P_3^{'} & 0.8 \le T \le 0.9 \\ P_4^{'} & 0.9 \le T \le 1.0 \end{cases} \tag{11}$$

Table 3. Trust rating table.

Trust Interval	Trust Level	Access Permission	Intensity of Permissions
[0,0.3]	distrust	null	refuse
(0.3,0.6]	less trusting	read	weak
(0.6,0.8]	basic trust	read, download	common
(0.8,0.9]	more trust	read, download, execute, update	strong
(0.9,1.0]	really trust	read, download, execute, update, delete	entire

5. Dynamic Updating Method of Trust Based on Authorization Feedback

5.1. Trust Dynamic Update Process

The feedback-based trust update is used after the access applicant obtains access permission through authorization. During and after accessing data resources, in order to manage and further control the behavior of access applicants during the whole process, the behavior of access applicants is periodically monitored and judged. According to the feedback of the trust evaluation factor, the current trust value is dynamically updated in real time, and the calculation result is used in the access control model. When the judgment knows that the subject may have performed illegal operations, the risk of trust value of the subject is evaluated from many aspects. Then, the results of the comprehensive evaluation are obtained in the form of feedback factors. The feedback factors are used to update the trust value of the previous cycle, and the updated result is applied to the permission adjustment, so as to manage and effectively control the behavior of the subject during the interaction process. This process starts when the subject is authorized and continues until the interaction is complete, which is shown in the Algorithm 1 below.

Algorithm 1 Trust Dynamic Update

```
establish connection
if complete authentication then
    gain historical trust value
    gain initial permission
    submit access request
    if submission of access request is compliant then
        obtain current trust value
        recalculate the trust value based on historical trust value
        normal exit
        forced exit
    end if
end if
forced exit
end
```

5.2. Trust Dynamic Update Method

5.2.1. Trust Evaluation Factor

Suppose the object is the data resource *i*, and the one evaluated is the access applicant *j* [25]. For *i*, the trust value of *j* is determined by *m* zero-trust evaluation indicators X= $\{X_1, X_2, \ldots X_m\}$.

The corresponding weight of each evaluation index to the trust value is $\omega' = \{\omega_{1'}, \omega_{2'}, \ldots, \omega_{m'}\}$, $\sum_{t=1}^{m} \omega_t^{'} = 1$, $1 \leq t \leq m$. t is the serial number of the evaluation index. The resource security level weight *g(i, j)* is introduced to divide the security levels of the data resource, $0 \leq g(i, j) \leq 1$. The value of *g(i, j)* is set according to the policy during the trust evaluation. The larger the value of *g (i, j)*, the higher the security level the data resource *i* is to the access applicant *j*.

Once authorized, in order to periodically evaluate the behavior of the subject, *i* will evaluate the trust of *j* against *m* evaluation indicators. The trust evaluation value $X_1, X_2, \ldots X_m$ for the evaluation indicators is $Y(X_t)$,$Y(X_t) \in [0, 1]$. The trust evaluation value of each index is compared with the historical experience value $\overline{Y_\mu(X_t)}$, and the subject's behavior is reflected through the trust evaluation factor $Z(X_t)$.

The historical experience value $\overline{Y_\mu(X_t)}$ is defined as the average value of the historical trust evaluation of the index X_t after μ times of interaction between *i* and *j*. That is, $\overline{Y_\mu(X_t)}$ represents the reference value for the evaluation of *j*'s trust value, and is expressed as follows:

$$\overline{Y_\mu(X_t)} = \frac{1}{\mu} \sum_{n=1}^{\mu} Y(X_n) \tag{12}$$

When the current trust evaluation value of $Y(X_t)$ is higher than $\overline{Y_\mu(X_t)}$, it indicates that subject *j* performs well in terms of indicators X_t in this interaction. The value of the trust evaluation factor corresponding to index X_t is $Z(X_t) \geq 1$, and plays a role in strengthening the trust of *j*. The difference between the trust evaluation value and the historical experience value is expressed as:

$$\Delta(X_t) = Y(X_t) - \overline{Y_\mu(X_t)},\ \Delta(X_t) \in [-1, 1] \tag{13}$$

The trust evaluation factor of the evaluation index X_t is defined as Equation (14).

$$Z(X_t) = \begin{cases} 0 & Z(X_t) \leq 0 \\ 1 + g(i, j)[Y(X_t) - \overline{Y_\mu(X_t)}] & others \end{cases} \tag{14}$$

When $\Delta(X_t)$ changes, the effect of resource security level weight *g (i, j)* on the trust update is verified, as shown in Figure 5.

5.2.2. Authorization Feedback Factor

By integrating the trust evaluation factors of m evaluation indicators, the overall evaluation of access applicant j for the data resource i is obtained, which is defined as the authorization feedback factor $\eta(i, j)$, $\eta(i, j) > 0$. $\eta(i, j)$ is used to characterize the trust evaluation of the interaction between *i* and *j*. First, the index weight ω' is obtained. Then, the authorization feedback factor is calculated, and the calculation formula is shown in Equation (15).

$$\eta(i, j) = \sum_{t=1}^{m} (\omega_t^{'} \times Z(X_{(t)})) \tag{15}$$

5.2.3. Trust Update

The authorization feedback factor is used to update the trust value of the data resource *i* to the access applicant *j*. The calculation Equation (16) is as follows, where $T^{'}(i, j, C)$ is the trust value before the update:

$$\mathrm{T}(i,j,C) = \begin{cases} 1 & (T^{'}(i,j,C) \neq 0) \wedge (\mathrm{T}(i,j,C) > 1) \\ \eta(i,j) \times \mathrm{T}^{'}(i,j,C) & (\mathrm{T}^{'}(i,j,C) \neq 0) \wedge (0 < \mathrm{T}(i,j,C) < 1) \end{cases} \tag{16}$$

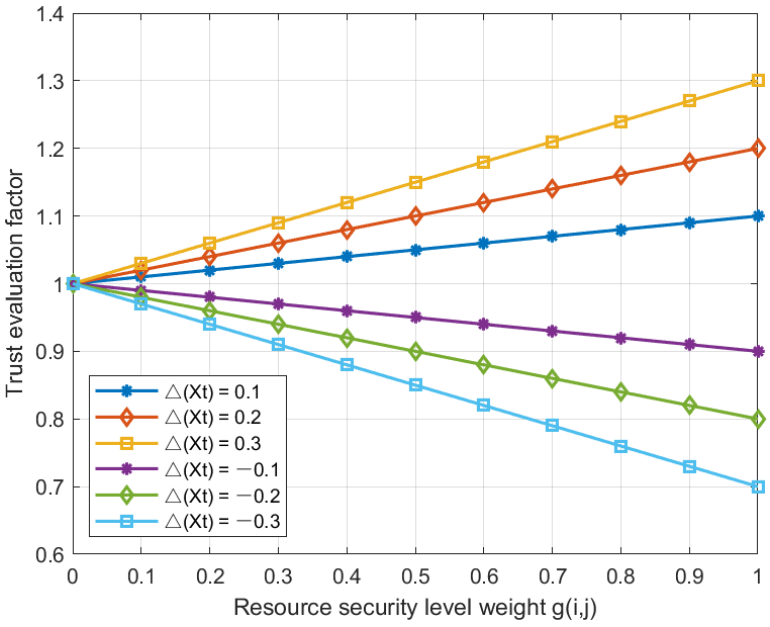

Figure 5. The relationship between trust evaluation factor and weight.

6. Real-Time Reliability Access Control Based on Rail Transit Data Platform

6.1. Rail Transit Data Platform

Intelligent transportation systems will further force traffic depth perception to increase, traffic information to be ubiquitous, traffic data to be pervasive, and traffic safety and efficiency to increase [29]. The overall planning of rail transit networks is generally divided into three regions: the production network, management network, and internet [30]. The division of the production network is divided into the production core network and production auxiliary network. The division of the management network is divided into production management network, OT security data collector logs, traffic data, security alarm data, collected user asset traffic logs, and other information. The management network realizes service management, organization management, asset management, vulnerability management, and alarm management service functions, and builds a basic information database, raw database, and knowledge database to provide data support for access authorization control. The information flow is shown in Figure 6.

Most of the traditional network security technologies adopt a static trust mechanism, which is no longer suitable for the current dynamic and complex network environment. It is necessary to change the entry point of the problem from the source to ensure that the participants of the rail transit data platform are trusted, so that the security of the entire complex network system can be ensured to a large extent. Therefore, the method of user behavior trustworthiness evaluation for complex network environments has become a research hotspot of network information security technology. Based on the idea of zero-trust dynamic continuous evaluation, a real-time trust calculation method was adopted, and the results were applied to the access control model.

6.2. Zero-Trust Measurement Index

The trust evaluation comprehensively considers multiple influencing factors of the access application context, that is, the zero-trust evaluation index is the collection of some subject attributes, object attributes, and environmental attributes related to the trust of the evaluation subject, including the subject authentication method (face recognition, account

password, and verification code), the current equipment location (outside the city, outside the city, in the station, or wherever the system equipment is located), the sensitivity level of resources (level 1, level 2, and level 3), access purpose (emergency, system operation and maintenance, financial transactions, and information query), access time (working hours and non-working hours), access method (system internal network, VPN, and public Wi-Fi), request frequency (too frequent, more frequent, general, and occasional), and blacklist (within and outside the blacklist), etc. Therefore, the evaluation of subject trust needs to take multiple influencing factors as evaluation indicators.

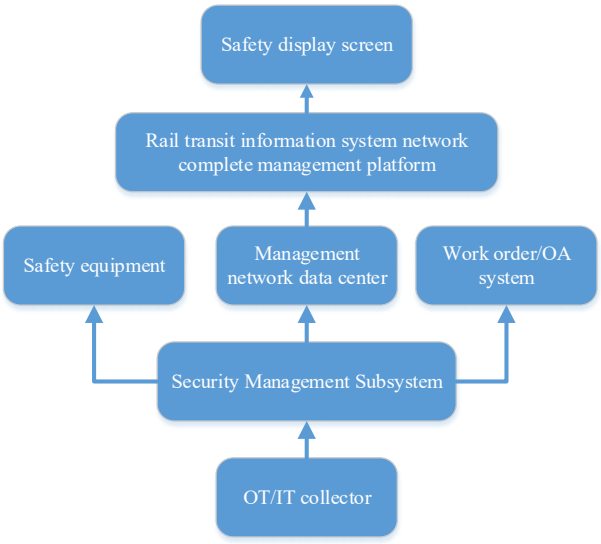

Figure 6. Information flow diagram of the system.

The zero-trust evaluation index is selected according to the national standard GB/t 22239–2019 basic requirements for network security classification protection of information security technology (hereinafter referred to as 'ISO 2.0') [31]. The network security level in China is divided into five levels, and the security requirements are enhanced step by step. The third level is applicable to important information systems. According to ISO 2.0, the security technical requirements of the protected object cover many control points at the levels of secure physical environment, secure communication network, secure area boundary, secure computing environment, security service operation center, etc. It consists of 10 zero-trust evaluation indicators, such as network architecture, communication transmission, border protection, access control, intrusion prevention, etc., as shown in Table 4.

Table 4. Zero-trust evaluation indicators.

Category	Project	Rating Setting (on a 100-Point Scale)	Value
Telecommunications and network security	Network architecture	(1) Legitimacy of equipment access ID; (2 points) (2) Black- and whitelist log registration; (2 points) (3) Effective interception of illegal access; (2 points) (4) Internal illegal access log registration; (2 points) (5) External illegal access log registration. (2 points)	10
	Port type	(1) Two-way TLS encryption; (3 points) (2) Access mode (internal network or not); (2 points) (3) Access the location of the equipment (whether inside the station); (2 points) (4) Two-way TLS decryption. (3 points)	10

Table 4. *Cont.*

Category	Project	Rating Setting (on a 100-Point Scale)	Value
Boundary of safe region	Perimeter security	(1) Access data flow monitoring; (3 points) (2) Instantaneous flow anomaly identification; (3 points) (3) External illegal abnormal access detection. (2 points)	8
	Access control	(1) Device IP acquisition under trust identification; (3 points) (2) Obtaining the IP address of the intercepted device; (3 points) (3) Application port on/off record; (2 points) (4) Purpose of the visit (whether it is urgent); (2 points) (5) Access time (whether during working hours); (2 points) (6) Sensitivity level of resources; (2 points) (7) Frequency of visits. (2 points)	16
	IDSIPS	(1) Security certificate certification; (4 points) (2) Internal network illegal access alarm; (4 points) (3) External network illegal access alarm. (4 points)	12
	Security audit	(1) Operation logs of system users; (2 points) (2) Abnormal login logs of security service operation center users; (2 points) (3) Network traffic audit logs. (4 points)	8
Security program to calculate the environment	Identification	(1) Login user identity identification; (2 points) (2) Multi-factor identity authentication. (2 points)	4
	Data integrity	(1) High-fidelity encryption and decryption of data transmission; (2 points) (2) Continuity of encrypted data traffic; (3 points) (3) Security anomaly event (ID time flow) record; (2 points) (4) Complete data transmission. (3 points)	10
	Material safety data sheet	(1) Two-way TLS encryption and decryption data; (3 points) (2) Access to files by the server of the security service operation center, audit of modification records, and operation alarm; (3 points) (3) Server file access and modification records. (2 points)	8
Security management center	Concentration supervisory control and management	(1) Centralized management of the full cycle of access control by the security service operation center; (2 points) (2) Obtaining the ID of system isolation equipment for security management; (4 points) (3) Log records of unsafe physical operations (device physical insertion and removal of USB/ network); (4 points) (4) CPU/ memory/disk space/traffic detection audit and operation alarm of the security service operation center server. (4 points)	14

At this time, m = 10. The scores are weighted by percentage, according to $\omega\ 1'$, $\omega\ 2'$, . . . , $\omega 10'$, which is the percentage of the project's score. For example, the value of $\omega\ 1'$ is 10%, which is the percentage of the network architecture's score. The satisfaction evaluation value of the evaluation index X_t is $Y(X_t)$. The calculation method is the ratio of the single score to the score of the project. Before calculation, each evaluation metric needs to be scored to determine whether the access is secure at this time. For example, the five metrics in the first project, network architecture, are legitimacy of equipment access ID, black- and whitelist log registration, effective interception of illegal access, internal illegal access log registration, and external illegal access log registration. The score of the network architecture is 10. If the five scoring items have a score of 1, 2, 2, 1, and 2, respectively, the value of $Y(X_1)$ is 8/10.

7. Conclusions

Most traditional rail transit data platforms take the user role as the center for access control. This paper introduces the zero-trust theory and makes a preliminary exploration on its application in the rail transit data platform. Zero-trust technology is used to solve the problem of network security threats in rail transit data platforms. According to the existing RBAC and ABAC models, this paper proposes an improved zero-trust-based fine-grained dynamic access control model. Combined with role-based access control, attribute-based access control, and trust-based access control, the induced ordered weighted average (IOWA) operator is applied to dynamically evaluate the trust value between visitors and accessed resources. Credibility is divided into five intervals. According to the risk feedback, the current trust level is dynamically updated in real time, and the results are used in the access control model. Taking rail transit as an example, this paper sets up ten relevant zero-trust evaluation indicators. Each trust measure is scored in a percentage system. Based on this model, related components can be promoted to realize fine-grained dynamic access control and protect the data resources and physical assets in the rail transit data platform. It is shown that the concept of zero trust can be applied practically by the preliminary application of rail transit.

In future research, qualitative and quantitative analysis of other characteristics of the model will be carried out, and measures will continue to be taken to improve and optimize all aspects of the access authorization control model, such as specifying the standards for setting parameter values during weight calculation. It is also important to clarify the policy details of the role evaluation and attribute evaluation phases based on the actual application scenarios. In addition, technologies such as the Internet of Things and blockchains also provide very good ideas for the security and dynamics of access control [32,33].

Author Contributions: Conceptualization, W.Y. and L.Z.; methodology, W.Y.; software, W.Y.; validation, W.Y.; formal analysis, W.Y.; investigation, W.Y. and L.Z.; resources, L.Z.; data curation, W.Y. and L.Z.; writing—original draft preparation, W.Y.; writing—review and editing, W.Y., L.Z., and Q.X.; visualization, W.Y.; supervision, L.Z.; project administration, L.Z.; funding acquisition, L.Z. All authors have read and agreed to the published version of the manuscript.

Funding: This work was sponsored by the Shanghai Science and Technology Innovation Action Program (No. 20511106400) and partly the by Shanghai Collaborative Innovation Research Center for Multi-network & Multi-modal Rail Transit.

Data Availability Statement: Not applicable.

Acknowledgments: We would like to thank Academician Jifeng He for his academic guidance and research contributions.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Xie, Z.; Liu, X.; Li, Y. Brief analysis of Network Security Scheme of Urban Rail Cloud Platform. *Netw. Secur. Technol. Appl.* **2020**, *11*, 124–126.
2. Gilman, E.; Barth, D. *Zero Trust Networks: Building Secure Systems in Untrusted Networks*; O'Reilly Media, Inc.: Sebastopol, CA, USA, 2017; pp. 15–30.
3. Xue, Y. *Research on Design of Security Framework Based on Zero Trust Architecture and Simulation Evaluation for Industrial Control System*; Lanzhou University of Technology: Lanzhou, China, 2022.
4. Zhang, Y. *Modifiable Blockchain Access Control Scheme Based on Dynamic Trust Evaluation Algorithm*; Shijiazhuang Tiedao University: Shijiazhuang, China, 2022.
5. Pan, R.; Wang, G.; Huang, H. Attribute Access Control Based on Dynamic User Trust in Cloud Computer. *Comput. Sci.* **2020**, *48*, 313–319.
6. John, K. No More Chewy Centers: Introducing the Zero Trust Model of Information Security. Available online: https://media.paloaltonetworks.com/documents/Forrester-No-More-Chewy-Centers.pdf (accessed on 4 January 2023).
7. Google, BeyondCorp. Available online: https://cloud.google.com/beyondcorp/ (accessed on 25 December 2022).
8. Zhang, H. Zero Trust Has Become a New Concept and Architecture of Cyber Security. Available online: http://www.jjckb.cn/2020-06/18/c_139147950.htm (accessed on 4 January 2023).

9. Shi, J. *Research on Security Defense Technology of Industrial Control Network Based on Zero Trust Mechanism*; North China Electric Power University: Beijing, China, 2022.
10. An Heng Information. An Integrated Intelligent Public Data Platform Security Protection System Based on Zero Trust Concept. Available online: https://c-csa.cn/case/case-detail/i-606/ (accessed on 4 January 2023).
11. Sangfor. Deep Trust Technology Group Comprehensive Zero Trust Security Practice. Available online: https://c-csa.cn/case/case-detail/i-640/ (accessed on 4 January 2023).
12. Chen, B.; Li, Y.; Gao, W. *Zero Trust Network Security: The Complete Guide to Software Defined Perimeter(SDP)*; Electronic Industry Press: Beijing, China, 2021; pp. 28–40.
13. Rose, S.; Borchert, O.; Mitchell, S.; Connelly, S. *Zero Trust Architecture*, 2nd ed.; NIST Special Publication 800-207; NIST: Gaithersburg, MD, USA, 2019.
14. Kamrun, N.; Asif, Q.; Terry, R. Developing an access control management metamodel for secure digital enterprise architecture modeling. *Secur. Priv.* **2021**, *4*, e160.
15. Qi An Xin. Zero-Trust Architecture and Solutions. 2020. Available online: http://www.caict.ac.cn/kxyj/qwfb/ztbg/202008/P020200812382865122881.pdf (accessed on 12 August 2020).
16. Xiong, H.; Zhang, B. Dynamic authorization-supported mechanism for grid. *Comput. Eng. Des.* **2011**, *32*, 9.
17. Zhang, Z.; Wang, P. Review of Zero Trust Security Architecture. *Secur. Sci. Technol.* **2021**, *131*, 8–16.
18. Liu, H. Zero trust security solution. *Green Alliance Technol. Zero Trust. Issue* **2020**, 40–43.
19. Zhang, Y.; Zhang, Y. A review of zero-trust research. *Inf. Secur. Res.* **2020**, *6*, 608–614.
20. Beth, T.; Borcherding, M.; Klein, B. *Valuation of Trust in Open Networks. European Symposium on Research in Computer Security*; Springer: Berlin, Heidelberg/Germany, 1994.
21. Tencent Zero Trust Security Solution Debut. Available online: https://baijiahao.baidu.com/s?id=1640736396843424663&wfr=spider&for=pc (accessed on 20 December 2022).
22. Bao, F.; Chen, I.R. Trust management for the internet of things and its application to service composition. In Proceedings of the 2012 IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM), San Francisco, CA, USA, 25–28 June 2012; pp. 1–6.
23. Singh, A.; Chatterjee, K. A multi-dimensional trust and reputation calculation model for cloud computing environments. In Proceedings of the 2017 ISEA Asia Security and Privacy (ISEASP), Surat, India, 29 January–1 February 2017; pp. 1–8.
24. Li, X.; Gui, X. Cognitive Model of Dynamic Trust Forecasting. *J. Softw.* **2010**, *21*, 163–176. [CrossRef]
25. Xiong, R. *Research on Key Technologies of Trust Based Grid Authorization*; PLA Information Engineering University: Zhengzhou, China, 2011.
26. Zhang, J.; Liu, B.; Sun, S.; Yu, W.; Zhang, L. Urban Rail Traffic Security Management System Based on Big Data Platform. In Proceedings of the IEEE 6th International Conference on Signal and Image Processing (ICSIP), Nanjing, China, 9–11 July 2021; pp. 1065–1069.
27. Yu, W.; Zhang, L. Research on Zero Trust Access Control Model and Formalization Based on Rail Transit Data Platform. In Proceedings of the IEEE the 10th International Conference on Information, Communication and Networks, Zhangye, China, 19–22 August 2022; pp. 689–695.
28. Zhang, B.; Xiong, R. Direct Trust Degree Evaluation Method Based on Authorization Feedback. *Comput. Eng.* **2012**, *38*, 163–166.
29. Zhang, L.; Shen, G.; Qin, X.; Cheng, C.; OU, D.; Li, X.; Shi, L. Information Physical Mapping and System Construction of Intelligent Network Transportation. *J. Tongji Univ. (Nat. Sci.)* **2022**, *50*, 79–86.
30. Chen, Q.; Gu, Y. Application of Mobile Payment in Urban Rail Transit AFC System. *Appl. Technol.* **2017**, *4*, 141–144.
31. Wang, Y.; Chen, L.; Yi, R. A new idea on network security protection of urban rail transit signal system in the era of classified protection 2.0. *Inf. Technol. Cyber Secur.* **2020**, *39*, 1–5.
32. Aftab, M.U.; Oluwasanmi, A.; Alharbi, A.; Sohaib, O.; Nie, X.; Qin, Z.; Ngo, S.T. Secure and dynamic access control for the Internet of Things (IoT) based traffic system. *PeerJ Comput. Sci.* **2021**, *7*, e471. [CrossRef] [PubMed]
33. Luo, J. *Research on Blockchain-Based Access Control Mechanism in Edge Computing*; Nanjing University of Posts and Telecommunications: Nanjing, China, 2022.