mathematics

MDPI

Article

Context-Aware Risk Attribute Access Control

Binyong Li [1,2,3,4], Fan Yang [1,*] and Shaowei Zhang [1]

[1] School of Cybersecurity, Xin Gu Industrial College, Chengdu University of Information Technology, Chengdu 610225, China; lby@cuit.edu.cn (B.L.); zsw_fy@163.com (S.Z.)
[2] Zhejiang Geely Holding Group, Hangzhou 310051, China
[3] Advanced Cryptography and System Security Key Laboratory of Sichuan Province, Chengdu 610225, China
[4] SUGON Industrial Control and Security Center, Chengdu 610225, China
* Correspondence: yangf_12@outlook.com

Abstract: Traditional access control systems exhibit limitations in providing flexible authorization and fine-grained access in the face of increasingly complex and dynamic access scenarios. This paper proposes a context-aware risk access control model to address these challenges. By developing a multi-level contextual risk indicator system, the model comprehensively considers real-time contextual information associated with access requests, dynamically evaluates the risk level of these requests, and compares the outcomes with predefined risk policies to facilitate access decisions. This approach enhances the dynamism and flexibility of access control. To improve the accuracy and reliability of risk assessments, we propose a combination weighting method grounded in game theory. This method reconciles subjective biases and the limitations of objective data by integrating both subjective and objective weighting techniques, thus optimizing the determination process for risk factor weights. Furthermore, smart contracts are introduced to monitor user behavior during access sessions, thereby preventing malicious attacks and the leakage of sensitive information. Finally, the model's performance and authorization granularity are assessed through empirical experiments. The results indicate that the model effectively addresses the requirements of dynamic and fine-grained access scenarios, improving the system's adaptability to risk fluctuations while safeguarding sensitive information.

Keywords: game theory-based weight assignment; risk assessment; adaptive access control

MSC: 68U01

Citation: Li, B.; Yang, F.; Zhang, S. Context-Aware Risk Attribute Access Control. *Mathematics* **2024**, *12*, 2541. https://doi.org/10.3390/math12162541

Academic Editors: Jianping Gou, Weihua Ou, Shaoning Zeng and Lan Du

Received: 28 June 2024
Revised: 12 August 2024
Accepted: 15 August 2024
Published: 17 August 2024

1. Introduction

The rapid advancement of information technology has rendered information security and privacy protection significant challenges for the contemporary society. Access control models serve as a fundamental mechanism for safeguarding the security of information systems and play a critical role in ensuring information integrity while maintaining user privacy. By limiting user access permissions, access control ensures that only authorized users can access necessary information, effectively enhancing security and mitigating risks. The evolution of communication technologies, such as 5G mobile networks, has resulted in increasingly complex and diversified resource access and usage scenarios, prompting a shift in access control mechanisms from static desktop environments to dynamic environments, including ubiquitous, cloud, and mobile computing settings. However, the development of access control technologies has lagged behind the evolving access demands. Traditional access control technologies, including Access Control Lists (ACLs), Mandatory Access Control (MAC), Discretionary Access Control (DAC), and Role-Based Access Control (RBAC), have somewhat protected system and resource security. Yet, in emerging access scenarios like cloud computing and the Internet of Things (IoT), these methods struggle to meet the requirements for flexible and fine-grained access control. On one hand, traditional

access control often employs static authorization methods in which user permissions remain unchanged over time, thereby failing to support fine-grained and dynamic access scenarios. On the other hand, traditional access control lacks contextual sensitivity, inhibiting the adjustment of user authorization policies in response to dynamically changing access environments, which compromises resource availability to some extent.

In view of the above problems, we propose a context-aware risk access control model and introduce a game theory-based portfolio weighting method in the risk assessment process. The main contributions of this paper are as follows:

(1) We propose a context-aware risk access control model that integrates multidimensional factors, including user identity, environmental context, and behavioral information. This model dynamically assesses the risk levels of access requests and facilitates flexible access control decisions based on this assessment.

(2) We introduce a combined weighting method based on game theory into the risk assessment process. By balancing both subjective and objective weighting methods, this approach enhances the accuracy and objectivity of risk assessments. After users obtain permissions, their activities during sessions are monitored through smart contracts. Upon detection of malicious behavior, user privileges can be reduced or sessions can be terminated, thereby realizing adaptive characteristics.

2. Related Work

To address the limitations of traditional access control methods in meeting dynamic access authorization requirements, researchers are increasingly proposing the use of security risk as a criterion for access authorization. By assessing the risk associated with access requests and evaluating their security implications, this approach, known as risk-based access control (RBAC, offers a more nuanced decision-making framework [1].

Cha et al. [2] introduced a risk-based evolutionary access control framework that adjusts user permissions based on the risk labels of data entities. Although access policies manage data access without risk labels, this framework lacks a quantitative method for assessing risk. Ke et al. [3] proposed a risk assessment scheme for fog nodes that determines access control through risk calculations involving subjects, objects, and contexts. Atlam et al. [4] introduced a Risk-based Neuro-Fuzzy System (NFS) model that evaluates risk using contextual information, thereby supporting dynamic access decisions based on real-time features. However, these models lack adaptive capabilities.

Shaikh et al. [5] incorporated trust and risk into access control mechanisms to facilitate dynamic authorization decisions. Yang et al. [6] proposed an adaptive weight allocation access control model, which dynamically assigns weights to risk assessment factors, thereby enhancing the accuracy of quantifying access control risks. Ding et al. [7] proposed a privacy-preserving multi-participant rational risk adaptive access control model. The model proposes a privacy quantization method for dynamic access datasets based on Shannon's self-information, and constructs an access request privacy risk function and a user privacy risk function so as to realize the adaptive risk level. With the advancement of medical information technology, medical information systems are increasingly utilized in diagnosis and treatment services [8]. Consequently, issues related to personal data and privacy protection have become critical in healthcare big data, necessitating urgent solutions [9,10]. Zhang et al. [11] constructed a dynamic risk-adaptive access control model that defines abnormal access behaviors for medical professionals and regularly updates risk scores and tolerance levels, thereby ensuring reliable access control in dynamic healthcare environments. Jiang et al. [12] created a new intuitionistic fuzzy trust access control model using a relative entropy-based intuitionistic fuzzy clustering algorithm and a reward and punishment mechanism to achieve adaptive and dynamic access control for physician access behavior.

A fundamental aspect of implementing risk-based access control is determining suitable risk assessment methods. Fuzzy risk analysis offers a viable solution for addressing uncertainty in risk evaluation. Recent research has begun integrating fuzzy logic into access

control to tackle the uncertainty and imprecision associated with risk [13]. Kesarwani et al. [14] proposed a subjective trust model for calculating trust values based on user and service provider behavior. Trust in resources is assessed by using a Mamdani fuzzy method with Gaussian and triangular affiliation functions for fuzzification and defuzzification and by employing parameters such as performance and resilience. Suleiman et al. [15] introduced a multi-level fuzzy inference system that employs fuzzy logic controllers to estimate risk. Zhang et al. [16] proposed an adaptive access control model based on context-awareness. The context-aware reasoning method based on fuzzy logic is used to evaluate the contextual scenario of user access, enabling the system to make special authorization decisions accordingly, and realizing the flexible and fine-grained authorization capability of the access control system in a dynamic environment. Shi et al. [17] proposed a fuzzy neural network-based risk quantification method that synthesizes risk information from subjects and objects using fuzzy theory, thereby reducing subjective bias in risk assessment. However, the existing risk assessment methods primarily calculate subjective or objective weights of risk indicators without considering the combined weights of these indicators.

To address the aforementioned issues, this paper builds upon attribute-based access control (ABAC) models and develops a context-aware risk access control model by analyzing the risk factors pertinent to access control. Compared to traditional access control technologies, ABAC [18–20] offers notable advantages in enhancing flexibility in access authorization. This model executes access authorization based on attributes present at the time of access requests, demonstrating high scalability and adaptability in dynamic and complex access environments. By establishing a multi-level contextual risk indicator system, this paper comprehensively considers real-time contextual information related to access requests, dynamically evaluates the associated risk levels, and compares these levels with predefined risk policies to inform access decisions. This approach significantly enhances the dynamism and flexibility of access control. To improve the accuracy and reliability of risk assessments, a combined weighting method based on game theory is proposed. By integrating both subjective and objective weighting methods, this approach balances subjective biases and deficiencies in objective data during the assessment process, optimizing the determination of risk factor weights to enhance the precision and reliability of risk evaluations. The risk assessment system calculates risk values and integrates them with risk access policies to achieve fine-grained user authorization. Once users obtain authorization, their behavior during access sessions is monitored using smart contracts to prevent malicious attacks and the leakage of sensitive information.

3. CARAC Access Control Model

With the rapid development and widespread adoption of information technology, secure access control has emerged as a core component of information system security. Traditional access control methods primarily rely on static identity authentication and permission management. However, given the increasing complexity of network environments and evolving security threats, access control based solely on static information is no longer adequate to address the multifaceted security challenges. In response to this backdrop, this paper proposes a context-aware risk attribute access control (CARAC) model. This access control model not only considers user identity and permissions but also integrates the environmental and behavioral contexts of access requests to dynamically assess and manage risk levels. Compared to traditional access control, context-aware risk access control exhibits greater dynamism and flexibility. By comprehensively considering user identity, environmental context, and behavioral information, the system can more accurately assess the risk levels of access requests and implement corresponding access control strategies based on actual circumstances.

3.1. Model Construction

As illustrated in Figure 1, the context-aware risk attribute access control (CARAC) model primarily consists of three components: the Context-awareness Module, the Risk

Assessment Module, and the Access Control Decision Module. This model determines access decisions by collecting real-time contextual information pertinent to access requests. Inputs to the model include user context, resource sensitivity, action sensitivity, and risk history. The Risk Assessment Module utilizes these inputs to assess the overall risk associated with each access request and compares this risk value against established risk policies to inform access decisions. Additionally, to detect abnormal user behavior, smart contracts are employed to track and monitor user activities throughout the entire access session, thereby preventing malicious attacks and the leakage of sensitive information.

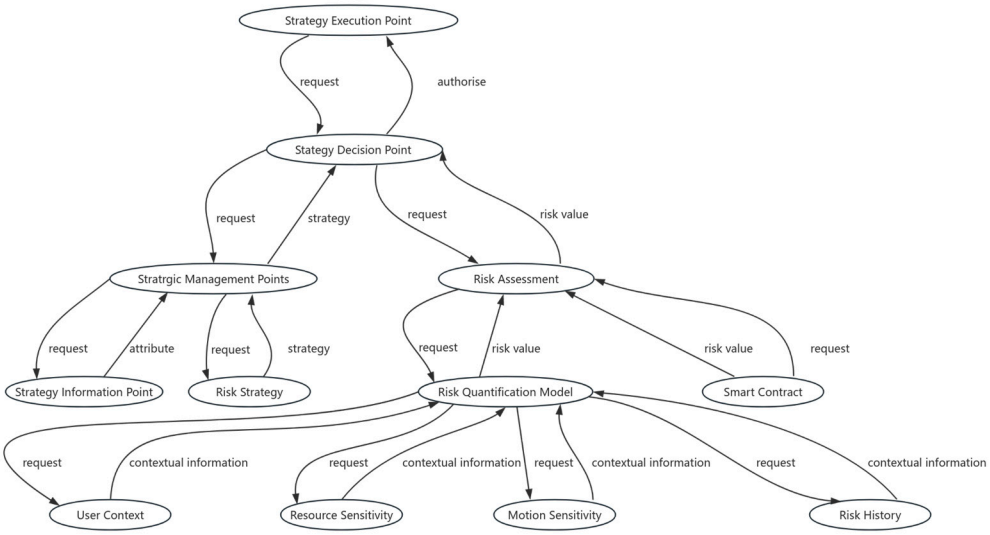

Figure 1. Context-aware to risk-based access control model.

Context awareness encompasses user-related contextual information within the system. Specifically, user context represents situational factors relevant at the time access requests are made, indicating risks associated with the requester, the application, and the access request itself. User context includes requester roles, access levels, physical locations, and system threat levels, among others. Resource sensitivity reflects the importance of the accessed resource, representing risks associated with the resource itself, including resource utilization and value. Action sensitivity denotes the impact of various actions on resource availability, integrity, and confidentiality, with higher sensitivity indicating a greater impact. Risk history describes the risk values of actions historically performed by users, allowing for the identification of behavioral patterns that may indicate malicious intent.

The Risk Assessment Module serves as the core component of the CARAC model. This module assesses the risk value of each access request based on input contextual risk factors, providing accurate risk evaluations in real-time context information to govern user access operations. Risk policies define the boundaries for permitted access and the conditions under which access may be granted or denied, determining the final access decision by comparing the assessed risk values with predefined policy thresholds. If the risk value of an access request is below the established risk policy threshold, access will be authorized.

3.2. Workflow Design of the Model

3.2.1. Model Workflow

The workflow of context-aware risk attribute access control is illustrated in Figure 2. Users initiate access requests to the Access Control Manager, specifying the resources or data they intend to access and the operations they wish to perform. Upon receiving the access request, the Access Control Manager employs context services to collect contextual information related to the user, including user context, the sensitivity level of the accessed resources, the sensitivity of the actions to be executed, and the user's risk history. The Risk

Assessment Module uses this information to evaluate the risk value of the access request, comparing it with predefined risk policies to inform the access decision.

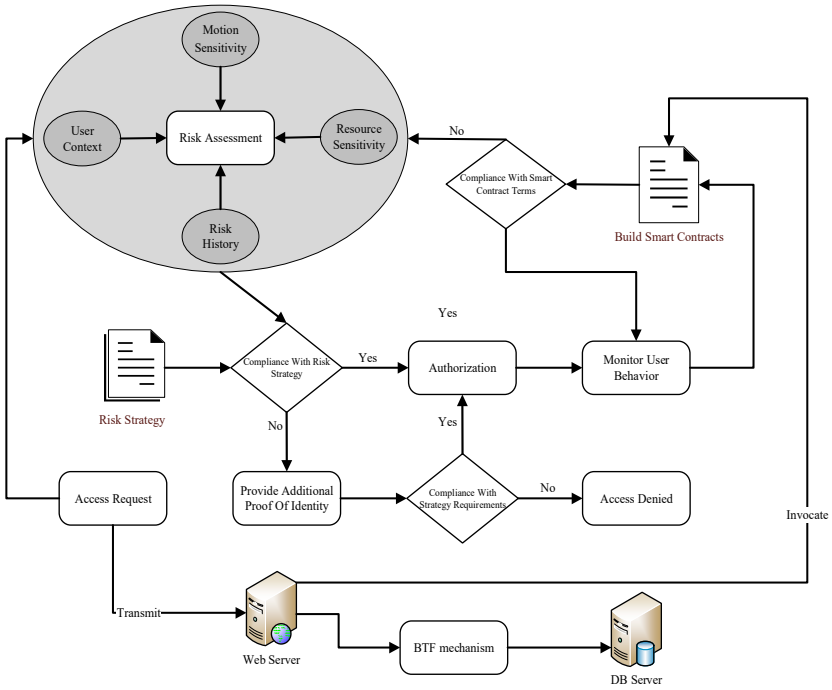

Figure 2. Model workflow.

Traditional access control authorizations are static, meaning that users' permissions remain fixed throughout the access process, which hinders the detection of malicious user behavior. Therefore, this model employs smart contracts to track and monitor user activities during access sessions following authorization, thereby enhancing the system's anomaly detection capabilities and flexibility. The Risk Assessment Module dynamically adjusts user permissions based on their behavior during these sessions; if anomalous behavior is detected, access can be restricted or terminated. If access is denied, users are prompted to provide additional identity verification to reduce false positives within the system. Upon receiving correct credentials, access is granted while the user session continues to be monitored.

3.2.2. Smart Contract Design

In order to realize the function of detecting access anomalies and provide adaptive capability for access control, this paper adopts smart contracts to track and monitor the activities during the user session to prevent malicious attacks and sensitive information leakage. The workflow of the smart contract is shown in Figure 3.

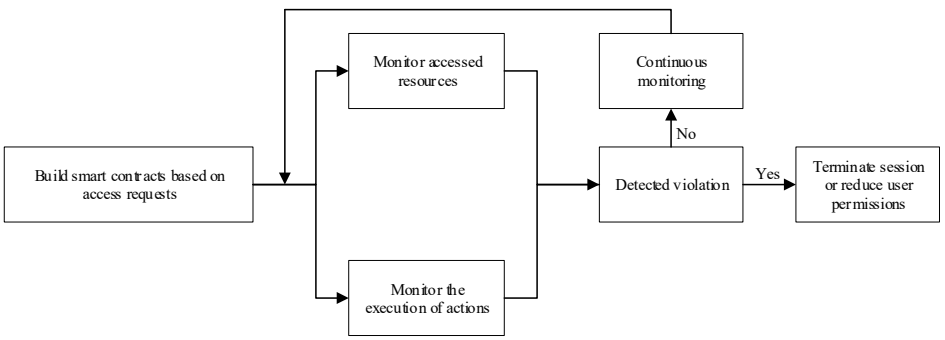

Figure 3. Behavior monitoring process.

When an access request is denied, the session is simply ended. If access is granted, a smart contract is used to track and monitor the user's activity during the access session to detect malicious behavior and ensure that the user complies with the terms and conditions of the smart contract. If the smart contract does not detect malicious behavior, it will continue to track and monitor the user's activity throughout the session. If a violation is detected, the system will immediately terminate the session or reduce the user's privileges and issue a warning.

3.2.3. Smart Contract Algorithm

To ensure that smart contracts can operate stably in unreliable network environments, Byzantine Fault Tolerance (BFT) is adopted as the core consensus mechanism. Byzantine Fault Tolerance is a highly secure consensus algorithm that maintains data consistency and service reliability even when up to one-third of the network nodes may exhibit malicious intent or failures.

The introduction of the BFT mechanism significantly improves the system's ability to defend against external attacks and internal threats, especially in the scenario of monitoring and controlling access behaviors, and enables it to respond quickly and accurately to various security events. By implementing this mechanism, the smart contract is able to reliably track and monitor user activities throughout the session, and once a violation is detected, the system can instantly take measures to terminate the session or adjust user privileges, thus ensuring data security and access compliance.

For user behavior monitoring, Algorithm 1 can be used. The system grants an initial authorization score to the user based on the user's authorization information, and also defines the corresponding action values for various possible violations. Once a user violation is detected during the user session, the system will update the authorization score based on the action values of the behavior. When the authorization score falls below the set threshold, the system updates the authorization information and adjusts the user privileges.

Algorithm 1. User Behavior Monitor

Input: *uid, permission, action*
Output: *Change permission*

Get *UserScores* from Permission
PermissionLevel ← *GetPermission (permission)*
    Get InitialValue
    InitialValue ← *PermissionLevel*
    UserScores ← *InitialValue*//*Grant users initial scores based on permissions*
Adjust *permissions* based on *user behavior*
    Define *behavior type* and *score*//*Define user behavior and action values*
    BehaviorType ← *GetAction(action)*
    CurrentScore = *UserScore*
    while (*CurrentScore* > *THRESHOLD*) **and then**
        CurrentScore ← *BehaviorScore*//*Update scores based on action values*
        if (*CurrentScore* == *UserScore*) **and then**
            Ignore the *event*//*The user score has not changed*
        else
            PermissionLevel ← *CurrentScore*
            Permission **update**
            return *Permission*//*Adjust permissions based on user scores*
        end if
    end while
Permission **update**//*Update user permissions*
return *Permission*

3.2.4. Model Utility Analysis

The smart contract used in this model is mainly used for real-time monitoring of user behavior. Meanwhile, the integration of the Byzantine Fault Tolerance (BFT) mechanism has improved the robustness and security of the system. This is specifically reflected in the following aspects:

(1) Initialize verification nodes: When deploying smart contracts, the system initializes a list of verification nodes. Each verification node is responsible for verifying user access requests and participating in the distributed decision-making process of the BFT mechanism.
(2) Receive access requests: Users submit access requests to smart contracts. The contract records each request through an event mechanism and triggers further verification processes.
(3) Verify request validity: Smart contracts use the BFT mechanism to verify user requests. Each verification node checks and evaluates requests to ensure they comply with access control policies. The BFT mechanism ensures consistency and security of the system in the event of partial node failures or attacks by conducting consistency checks among multiple validation nodes.
(4) Granting or denying access permissions: Based on the verification results of the BFT mechanism, smart contracts determine whether to grant user access permissions. If the majority of verification nodes confirm that the request is valid, the contract will grant access and record this operation. If the request is rejected, the contract will block user access and record the reason for the rejection.
(5) Real time monitoring and adjustment: Smart contracts continuously monitor user behavior during user sessions. The BFT mechanism ensures that the system can dynamically adjust access control policies to address potential security threats or abnormal behavior. Once abnormal user behavior is detected, smart contracts will automatically take measures, such as adjusting user permissions or terminating sessions, to prevent data leakage or other security risks.
(6) System adaptability and flexibility: Through the BFT mechanism, smart contracts enhance their adaptability and flexibility to abnormal situations. Even under extreme conditions such as node failures or malicious attacks, the BFT mechanism maintains stability and consistency through a distributed verification process, thereby enhancing the overall security and reliability of the system.

Smart contracts play an indispensable core role in the risk access control model proposed in this section. By accurately and automatically executing preset rules and conditions, smart contracts not only significantly improve the response speed and processing accuracy to security threats, but also achieve real-time monitoring and continuous evaluation of user behavior. As shown in Figure 3, smart contracts can detect and identify potential violations or malicious activities in a timely manner. Once they discover that user behavior may violate security policies, they will immediately take measures, including but not limited to terminating the session or adjusting user permissions, in order to effectively prevent data leakage or other security risks from occurring.

Moreover, smart contracts, through distributed execution between different nodes, not only enhance the system's resistance to single point failures, but also ensure that even if some system components are attacked or fail, other parts of the system can still maintain normal operation, ensuring the stability and continuity of the entire system. This adaptive capability enables smart contracts to dynamically adjust access security measures based on real-time data and user behavior, greatly improving the efficiency and effectiveness of access control models. Through this approach, smart contracts ensure that critical operations of the system remain stable and secure even under extreme conditions, enhancing the overall resilience and reliability of the system.

4. Risk Perception Based on a Game Theory-Based Weight Assignment Method

Risk assessment plays a crucial role in risk-adaptive access control mechanisms by identifying and filtering threats and abuses that may arise during the access control process. Establishing a scientific, efficient, and standardized risk assessment system is essential for the real-time and dynamic identification of potential risks at each stage, thereby supporting secure access control strategies and facilitating the effective allocation of access permissions. By setting clear risk assessment objectives and selecting appropriate assessment methods, the scientific rigor and efficiency of risk assessment can be enhanced. This process involves analyzing attributes and their interactions within the access control framework, scientifically predicting risk impacts, and selecting suitable assessment strategies based on practical application requirements.

4.1. Establishment of Risk Indicators

When quantifying risks, it is essential to consider various risk attributes associated with access, as each attribute serves as an evaluation criterion. To comprehensively assess risks during user access, this study constructs a risk assessment framework that incorporates user context factors (subject risk), historical context factors (historical risk), action context factors (behavioral risk), and resource context factors (object risk), as illustrated in Figure 4.

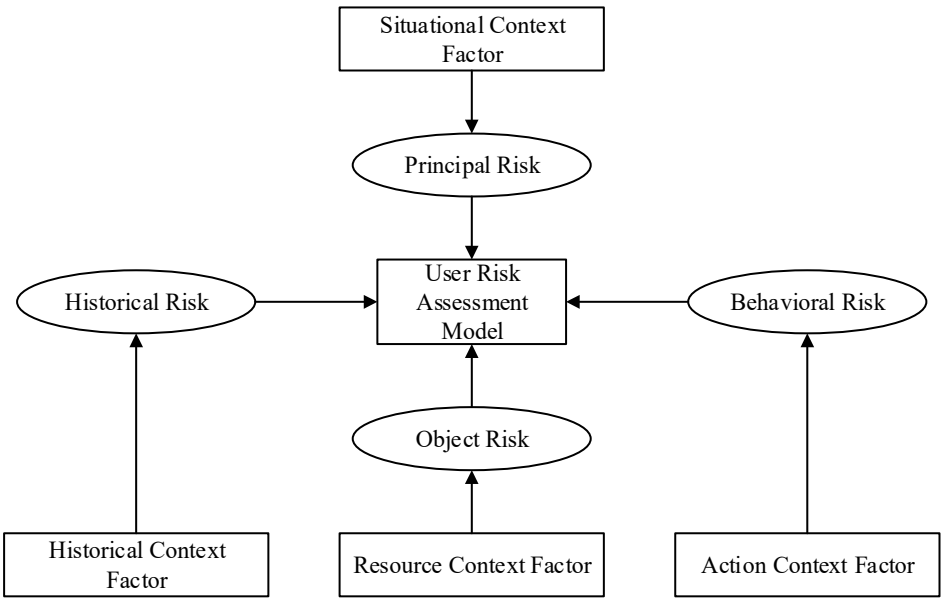

Figure 4. Risk assessment system.

Based on the membership relationship between risks and different risk attributes, all attributes can be abstracted into the form of an attribute tree. The attribute tree is structured into three levels: the top level is the objective layer, containing a single root node; the middle level comprises first-level indicators, including user context, resource sensitivity, action sensitivity, and risk history; and the bottom level consists of second-level indicators that encompass various specific attributes.

Figure 5 depicts the risk assessment factor system, with the following explanations for each factor.

Resource context refers to the attributes of resources and uses resource sensitivity to describe the importance and sensitivity of resources within the system. In this paper, resource sensitivity is measured using resource utilization, resource quality, and resource value.

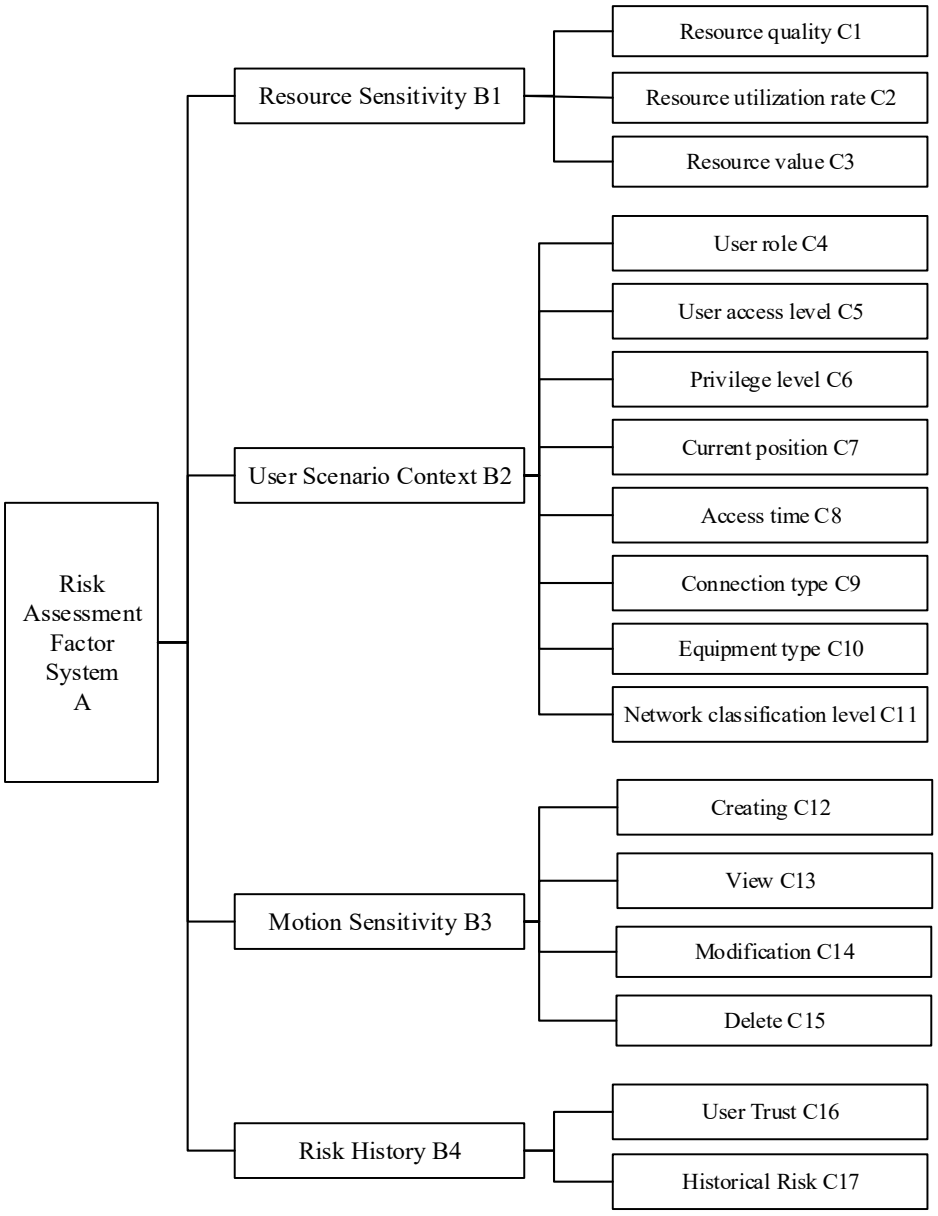

Figure 5. Risk assessment factors.

Resource utilization: The likelihood of resource misuse increases with its frequency of use, indicating a higher degree of resource sensitivity. Resource utilization is calculated using the following formula:

$$p(R_i) = \frac{\sum_{i=1}^{m} C_{U_i,D_j}}{\sum_{j=1}^{k}\sum_{i=1}^{m} C_{U_i,D_j}} \tag{1}$$

In the formula, U_i represents a user i, D_j represents a resource j, $\sum_{i=1}^{m} C_{U_i,D_j}$ denotes the number of times user i accesses data resource D_j, and $\sum_{j=1}^{k}\sum_{i=1}^{m} C_{U_i,D_j}$ denotes the total number of times all data resources are accessed.

Resource Quality: This factor represents the proportion of missing or erroneous data relative to correct data within a resource. The higher the resource quality, the more sensitive the resource becomes. Resource quality is calculated using the following formula:

$$p(R_i) = \frac{\frac{\sum_{s_r} co(R_j)}{s_r}}{\sum_{i=1}^{n} \frac{\sum_{s_i} co(R_i)}{s_i}} \quad (2)$$

In the formula, $co(R_i)$ represents the number of correct data items in all data items R_i within a resource, s_i represents the total number of data items R_i in the resource, $\frac{\sum_{s_r} co(R_j)}{s_r}$ represents the proportion of correct data items in a single resource, and $\sum_{i=1}^{n} \frac{\sum_{s_i} co(R_i)}{s_i}$ represents the total number of correct data items in all resources.

Resource Value: Owners or managers of resources evaluate the value of their resources using professional assessment methods.

User Contextual Scenario: This describes the contextual factors related to user access requests, which can be categorized into three main areas. First, there are identity-related risk factors, including the user's role in the system, user access level, and user permission level. Second, intermediary component-related risk factors come into play, such as the type of device used when requesting access, the network classification level used to establish the connection, and the connection type. Lastly, the real-world context in which the user is situated is considered, including location information and time details at the moment access is requested.

Action Sensitivity Description: This describes the extent to which user actions or operations in specific environments or contexts affect system security, privacy, and other aspects. It is used to assess and manage the potential risks associated with various operations on the system. Different actions pose varying degrees of risk to resource availability, integrity, and confidentiality. The impact of actions on resource risk value depends on resource attributes and is typically evaluated based on the likelihood of threats and potential impacts. The correlation between different user actions and resource sensitivity, along with their associated risk scores, is shown in Table 1.

Table 1. Action risk values.

Title 1 Action	Resource Sensitivity	Title 2 Action Risk Value		
		Availability	Integrity	Confidentiality
Create	Sensitive/not sensitive	1	1	0
View	Sensitive	0	0	1
	Not sensitive	1	0	0
Modify	Sensitive/not sensitive	1	1	0
Delete	Sensitive/not sensitive	1	1	0

Viewing resources typically does not impact their integrity; however, accessing sensitive resources can affect their confidentiality. Therefore, the ratings in Table 1 differentiate between these actions. The ratings regarding the impact of various actions on resources are determined based on the sensitivity of the resources.

Risk history refers to the risk characteristics and records of risk exhibited by users in their past behaviors and activities. It is assessed through the risk values associated with users' historical accesses and their trustworthiness.

4.2. Combination Weighting Method Based on Game Theory

Risk assessment methods are primarily categorized into subjective weighting methods and objective weighting methods. Subjective weighting methods rely on the personal judgments of assessors and are currently the most widely used approach. This method leverages the assessors' experience and knowledge to subjectively evaluate the relative importance of indicators, emphasizing individual perspectives and experiences, thus providing personalized ratings. However, this reliance on expert judgments can result in overlooking influential factors related to the events themselves, as it may lack objective data support and lead to biased outcomes. In contrast, objective weighting methods are based on objective data and standards, characterized by strong mathematical theoretical foundations, objectivity, and repeatability. From a mathematical standpoint, data-driven methods produce assessment results that are more scientific and accurate. However, such methods require clear numerical characteristics of the assessment objects for modeling, may lack expert judgment on the indicators, and can neglect individual differences and specific circumstances.

To address these limitations, this paper proposes a combined weighting method based on game theory that integrates the advantages of both subjective and objective weighting approaches to establish the weight basis of various factors affecting access risk. By introducing the theoretical framework of game theory, participants are regarded as rational decision-makers, quantifying the weight of different factors affecting access risk through a combination of expected values and probability. This method comprehensively considers the interests and behavioral strategies of all parties, effectively balancing subjective and objective factors, and providing a more rational basis for weight distribution—ultimately yielding more credible and accurate risk assessment results. Figure 6 illustrates the process of risk perception through combined weighting informed by game theory.

4.2.1. Subjective Weighting Method—Analytic Hierarchy Process (AHP)

The Analytic Hierarchy Process (AHP) is a multi-criteria decision-making technique that decomposes decision problems into multiple hierarchical levels. It employs comparison matrices and weight calculations to evaluate and contrast factors layer by layer, thereby determining the distribution of weights.

During the assessment, risk evaluation factors are categorized into three layers: the objective layer, the criteria layer, and the decision layer. After establishing the hierarchical structure, the relative importance among factors within each layer is assessed and quantified using data, resulting in a hierarchical judgment matrix.

Taking the first-level risk indicators of user context B_1, resource sensitivity B_2, action sensitivity B_3, and risk history B_4 as examples, set their importance values to a, b, c and d, respectively, and form a judgment matrix. Taking B_1, B_2, B_3 and B_4 as the rows and columns of the judgment matrix, set the elements within the matrix to a_{ij}.

$$s_{ij} = \frac{s_i}{s_j} \tag{3}$$

In the formula, s_i represents the importance value of primary risk indicator B_i, s_j represents the importance value of primary risk indicator B_j. $i, j = 1, 2, \ldots, n, (n = 4)$, i and j represent the row and column of the judgment matrix, and Table 2 shows the judgment matrix:

Table 2. Judgment Matrix.

$\frac{s_i^{\#}}{s_j}$	**User Scenario B_1^***	**Resource Sensitivity B_2**	**Action Sensitivity B_3**	**Risk History B_4**
User Scenario B_1	1	$\frac{a}{b}$	$\frac{a}{c}$	$\frac{a}{d}$
Resource Sensitivity B_2	$\frac{b}{a}$	1	$\frac{b}{c}$	$\frac{b}{d}$
Action Sensitivity B_3	$\frac{c}{a}$	$\frac{c}{b}$	1	$\frac{c}{d}$
Risk History B_4	$\frac{d}{a}$	$\frac{d}{b}$	$\frac{d}{c}$	1

*B B, the primary risk indicator. # s, the importance value of primary risk indicator B.

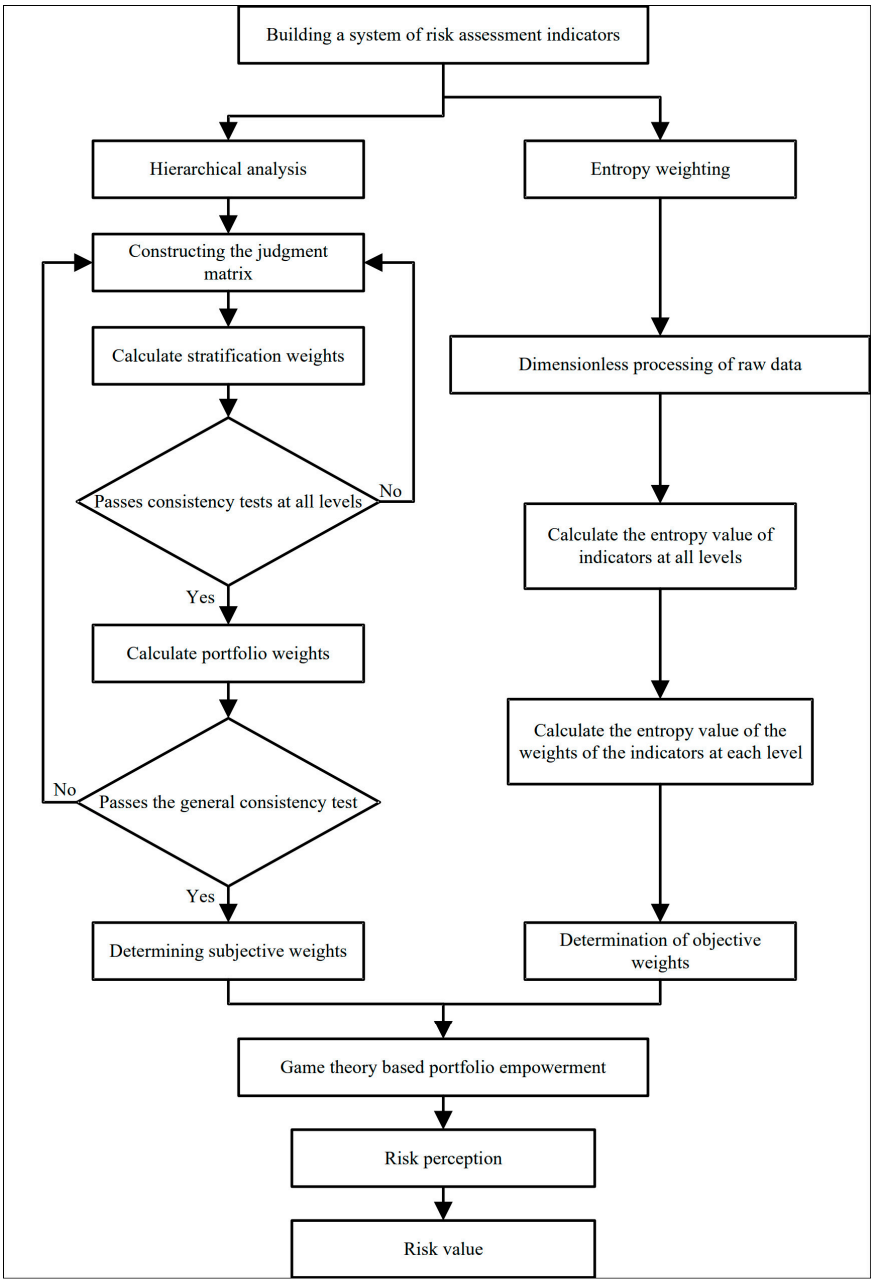

Figure 6. Risk perception process.

According to the judgment matrix table, an nth order judgment matrix is obtained:

$$S = \begin{bmatrix} s_{11} & s_{12} & \cdots & s_{1n} \\ s_{21} & s_{22} & \cdots & s_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ s_{n1} & s_{n2} & \cdots & s_{nn} \end{bmatrix}$$

Before calculating the weights, it is necessary to perform a consistency test on the judgment matrix, first calculating the consistency index CI:

$$CI = \frac{\lambda_{\max} - n}{n - 1} \tag{4}$$

Find the corresponding average random consistency index RI, and calculate the consistency ratio CR:

$$CR = \frac{CI}{RI} \tag{5}$$

Normalize the data within the judgment matrix, and sum the normalized judgment matrix row by row to obtain vector $\overline{W} = \left(\overline{W}_1, \overline{W}_2, \cdots, \overline{W}_n\right)^T$.

$$\overline{W}_i = \sum_{j=1}^{n} s_{ij}, (i, j = 1, 2, \cdots, n) \tag{6}$$

Normalize vector $\overline{W} = \left(\overline{W}_1, \overline{W}_2, \cdots, \overline{W}_n\right)^T$.

$$W_i = \frac{\overline{W}_i}{\sum_{j=1}^{n} \overline{W}_j}, (i = 1, 2, \cdots, n) \tag{7}$$

Obtain the weight vector $W_B = (w_1, w_2, \cdots, w_n)^T$ for the first-level risk indicators.

4.2.2. Objective Weighting Method—Entropy Weighting Method

To determine the objective weights of access risk factors, the entropy weighting method is utilized for evaluation. The entropy weighting method is a weight calculation technique based on the principle of information entropy, commonly employed for multi-criteria comprehensive evaluations or for solving optimal decision-making problems. The weights of indicators can be derived from real data, with weights assigned to each indicator based on its calculated information entropy. The smaller the information entropy of an indicator, the more information it provides, and, consequently, the greater its weight. The calculation steps are as follows:

Step 1: Since the measurement units and dimensions of different indicators vary, the data must first be standardized to unify dimensions and magnitudes, thereby eliminating the influence of unit differences on the calculation results. The standardization formula is as follows:

$$\sigma_i = \sqrt{\frac{\sum_{i=1}^{m} \left(x_{ij} - \overline{x}_{ij}\right)^2}{m}} \tag{8}$$

$$x'_{ij} = \frac{x_{ij} - \overline{x}_{ij}}{\sigma_i} \tag{9}$$

In the formula, σ_i is the standard deviation of the indicator, $\overline{X}_{ij}$ is the mean of the indicator, where x'_{ij} is the standardized raw data of the j-th indicator on the i-th risk factor.

Step 2: When the original data contain negative values, direct calculations may yield inaccurate or ambiguous results. To address this issue, the coordinate translation method can

be employed by adding a constant to all data points. This approach eliminates the influence of negative values on the calculation results derived from the aforementioned formula.

$$p_{ij} = x'_{ij} + z \tag{10}$$

In the formula, where p_{ij} is the value after using the coordinate translation method, Z is the shift magnitude.

Step 3: Calculate the probability P_{ij} of the j-th indicator occurring in the i-th sample.

$$p_{ij} = \frac{x_{ij}}{\sum\limits_{i=1}^{m} x_{ij}} (i = 1, 2, \cdots, m; j = 1, 2, \cdots, n) \tag{11}$$

Step 4: Calculate the entropy value e_j of the j-th indicator using the information entropy formula based on the probability value.

$$e_j = -k \sum_{i=1}^{m} p_{ij} In p_{ij} (j = 1, 2, \cdots, n), k = 1/Inm \geq 0, e_j \geq 0 \tag{12}$$

Step 5: Calculate the coefficient of variation g_i for the j-th indicator.

$$g_i = 1 - e_j (j = 1, 2, \cdots, n) \tag{13}$$

Step 6: Calculate the weight w_j of the j-th indicator.

$$w_j = \frac{g_j}{\sum_{j=1}^{n} g_j} (j = 1, 2, \cdots, n) \tag{14}$$

Step 7: Calculate the coefficient of variation value for each criterion-level indicator based on the coefficient of variation g_j of the lower-level structural indicators, denoted as $G_k, k = 1, 2, \cdots, N$, where N is the number of layers in the criterion level, and the coefficient of variation reflects the relative dispersion of criterion-level indicators compared to lower-level structural indicators. The formula for calculating the coefficient of variation can be expressed as

$$G_k = \sum_{j=1}^{n} \frac{g_j \times w_j}{N} \tag{15}$$

Step 8: Determine weight values:

$$w_k = \frac{G_k}{\sum\limits_{k=1}^{N} G_k}, (k = 1, 2, \cdots, N) \tag{16}$$

4.2.3. Comprehensive Empowerment Method

The combination weighting approach grounded in game theory integrates weights derived from various weighting methods. Utilizing game theory to compute combined weights entails identifying a balance point that optimizes the interests of both parties. Through the analysis and reconciliation of conflicts among different weighting methods, this approach minimizes the disparity between subjective and objective weights. This article takes the subjective weight $W_1 = (w_{11}, w_{12}, \cdots, w_{1n})$ based on the Analytic Hierarchy Process (AHP) as one party of the game, and the objective weight $W_2 = (w_{21}, w_{22}, \cdots, w_{2n})$ determined based on the entropy method as the other party of the game, to solve the optimal weight combination.

Step 1: Construct the linear combination weight W of W_1 and W_2.

$$W = \begin{bmatrix} \alpha w_{11} + \beta w_{21} \\ \alpha w_{12} + \beta w_{22} \\ \vdots \\ \alpha w_{1n} + \beta w_{2n} \end{bmatrix} = \begin{bmatrix} w_{11} & w_{21} \\ w_{12} & w_{22} \\ & \vdots \\ w_{1n} & w_{2n} \end{bmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \alpha w_1 + \beta w_2 \tag{17}$$

where n is the number of evaluation indicators, and α and β are the linear combination coefficients of W_1 and W_2, respectively.

Step 2: To minimize the discrepancy between the combined weight W and W_1 and W_2, the optimal linear combination coefficients α^* and β^* are solved. The combination weight at this time is the optimal combination weight W^*.

$$\begin{gathered} \min(||W - W_1||_2 + ||W - W_2||_2) = \\ \min(||\alpha W_1 + \beta W_2 - W_1||_2 + ||\alpha W_1 + \beta W_2 - W_2||_2) \end{gathered} \tag{18}$$

According to the properties of matrix differentiation, the optimal first-order derivative condition is

$$\begin{cases} \alpha W_1 W_1^T + \beta W_1 W_2^T = W_1 W_1^T \\ \alpha W_2 W_1^T + \beta W_2 W_2^T = W_2 W_2^T \end{cases} \tag{19}$$

Using Matlab software 9.13 to solve the linear combination coefficients α and β, and then normalizing them, the optimal combination weight of the evaluation indicators is obtained as $W^* = \alpha^* W_1 + \beta^* W_2$, and α^* and β^* are the optimal linear combination coefficients of W_1 and W_2, respectively.

4.3. Perceive the Risks of the System

Weights for the factors of the risk assessment system developed in this paper are allocated, as demonstrated in Table 3.

Table 3. Risk factor weight.

Criterion Level	Subjective Weights	Objective Weights	Portfolio Weights	Indicator Level	Subjective Weights	Objective Weights	Portfolio Weights
User scenario	0.3724	0.4126	0.4239	User role	0.0384	0.0415	0.0417
				User access level	0.0539	0.0573	0.0575
				Privilege level	0.1419	0.1746	0.1765
				Current position	0.1749	0.2014	0.2029
				Access time	0.1458	0.1529	0.1533
				Connection type	0.1351	0.0946	0.0923
				Equipment type	0.1518	0.1153	0.1132
				Web classification level	0.1582	0.1624	0.1626
Resource sensitivity	0.1548	0.1739	0.1794	Resource utilization rate	0.3825	0.3139	0.4001
				Quality of resources	0.1385	0.1847	0.1266
				Resource value	0.4791	0.5014	0.4734
Motion sensitivity	0.2155	0.2274	0.2311	Establish	0.0605	0.0452	0.0831
				View	0.1034	0.1346	0.0573
				Modify	0.3157	0.3584	0.2526
				Delete	0.5204	0.4618	0.6069
Risk history	0.2573	0.1851	0.1656	Historical risk values	0.5484	0.5059	0.5544
				User confidence	0.4516	0.4941	0.4456

Following the acquisition of combined weights for the risk indicators, a risk assessment for access authorization and adaptive features is performed by gathering contextual data during user-initiated access requests and user sessions. The steps involved in user risk assessment are outlined as follows:

Taking resource sensitivity as an example, at a specific moment, the scores for resource utilization rate, resource quality, and resource value are recorded as 0.514, 0.767, and 35.8, respectively.

Step 1: Constructing a fuzzy comment set. The evaluation factors for resource sensitivity include resource utilization rate, resource quality, and resource value. A fuzzy comment set is constructed based on these scores.

$$V = \{v_1, v_2, v_3, v_4\} = \{low, medium, high, very\ high\}$$

where $\{v_1, v_2, v_3, v_4\}$, respectively, represent the judgment criteria for resource utilization rate, resource quality, and resource value as "low", "medium", "high", and "very high".

Step 2: Constructing membership functions. The construction of membership functions should be based on the characteristics of various evaluation factors. It is essential to align the creation of these functions with the security standards mandated by different organizations.

The membership function defined for the resource utilization rate is illustrated in Figure 7.

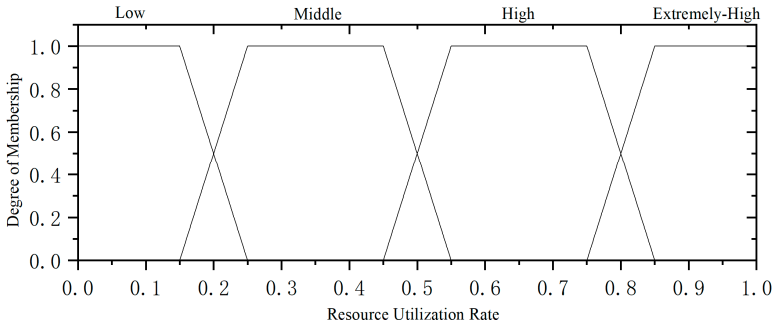

Figure 7. Resource utilization affiliation function.

Similarly, membership functions for resource quality and resource value are defined, and these are presented in Figures 8 and 9, respectively:

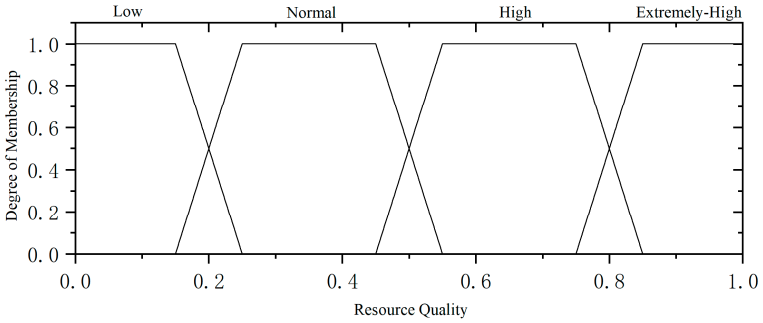

Figure 8. Resource quality affiliation function.

Step 3: Performing fuzzy comprehensive evaluation on each risk factor separately to obtain the degree of membership of the risk factor to the n comment v_n in the fuzzy comment set. By collecting contextual information from the system, the resource value score, resource utilization score, and resource quality score are input into their respective membership functions to obtain fuzzy evaluation results.

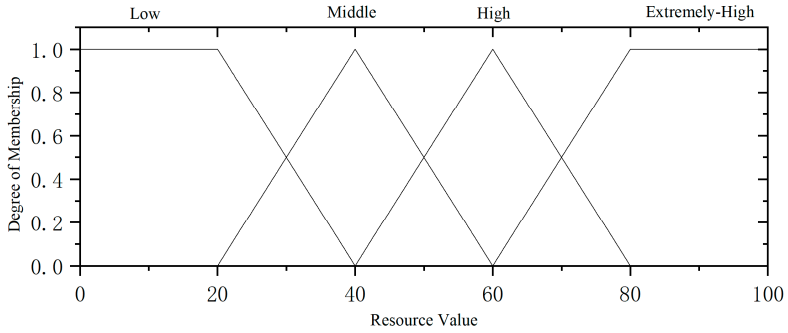

Figure 9. Resource value affiliation function.

The membership degree for the resource utilization rate is as follows:

$$V_{C_9} = \{0,\ 0.36,\ 0.64,\ 0\}$$

The membership degree of resource quality is as follows:

$$V_{C_{10}} = \{0,\ 0,\ 0.83,\ 0.17\}$$

The membership degree of resource value is as follows:

$$V_{C_{11}} = \{0.21,\ 0.79,\ 0,\ 0\}$$

Step 4: Constructing a fuzzy evaluation matrix R.

$$R_{B_2} = \begin{pmatrix} 0 & 0.36 & 0.64 & 0 \\ 0 & 0 & 0.83 & 0.17 \\ 0.21 & 0.79 & 0 & 0 \end{pmatrix}$$

Step 5: Calculating the fuzzy evaluation results for resource sensitivity.

$$V_{B_2} = W_{B_2} \circ R_{B_2} = (0.4001\ 0.1266\ 0.4734) \begin{pmatrix} 0 & 0.36 & 0.64 & 0 \\ 0 & 0 & 0.83 & 0.17 \\ 0.21 & 0.79 & 0 & 0 \end{pmatrix}$$
$$= (0.099\ 0.518\ 0.293\ 0.022)$$

Step 6: Repeating Steps 1 through 5 to calculate the evaluation results V_{B_1}, V_{B_3} and V_{B_4} for user context, action sensitivity, and risk history, respectively. Combine these to form the first-level risk indicator evaluation matrix.

$$R_A = \begin{pmatrix} 0.218 & 0.143 & 0.381 & 0.258 \\ 0.099 & 0.518 & 0.293 & 0.022 \\ 0.184 & 0.366 & 0.245 & 0.205 \\ 0.649 & 0.127 & 0.047 & 0.177 \end{pmatrix}$$

Step 7: Calculating the user risk score.

$$V_A = W_A \circ R_A = (0.4239\ 0.1794\ 0.23011\ 0.1657) \begin{pmatrix} 0.218 & 0.143 & 0.381 & 0.258 \\ 0.099 & 0.518 & 0.293 & 0.022 \\ 0.184 & 0.366 & 0.245 & 0.205 \\ 0.649 & 0.127 & 0.047 & 0.177 \end{pmatrix}$$
$$= (0.260\ 0.259\ 0.278\ 0.190)$$

A context-aware risk-based access control model identifies risk factors during user access, constructs a risk assessment indicator system, and utilizes this system as input for a

risk assessment algorithm. This model dynamically perceives risk throughout the user's access period, thereby providing a basis for access authorization.

The framework of the context-aware risk-based access control model is illustrated in Figure 10. This model primarily comprises three core components: risk assessment, access decision, and smart contract. The risk assessment component evaluates risks during the access period, while the access decision component utilizes the assessment results as a basis for authorization, granting permissions according to predefined access policies. Upon authorization, a smart contract is created for the user. If user attributes, status, or contextual conditions change, or if the user breaches the terms of the smart contract, the system promptly terminates the session, reduces the user's privileges, and issues a warning.

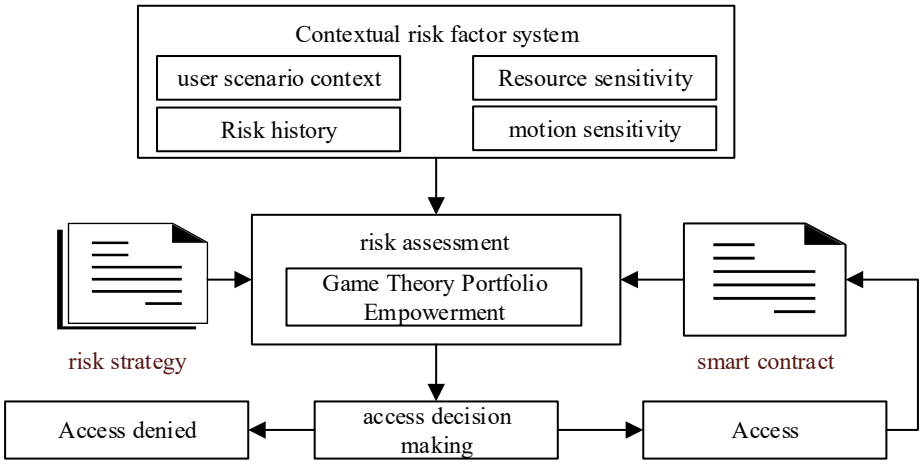

Figure 10. Access control framework.

5. Experimental Analysis

This paper presents a prototype system developed from the discussed access control model and outlines experiments designed to evaluate its usability and performance. The experimental test environment is configured on a 64-bit Windows 11 operating system, featuring an AMD Ryzen 5 5600G octa-core processor which from Advanced Micro Devices, Inc. in Santa Clara, CA, USA, 16 GB of RAM, and PyCharm 2022 as the integrated development environment. Experiments were conducted to compare the time costs associated with context-aware risk-based access control (CARAC) and attribute-based access control (ABAC) during the decision-making and authorization processes, thereby assessing their performance.

As illustrated in Figure 11, the context-aware risk-based access control (CARAC) model enhances attribute-based access control by incorporating a risk assessment authorization mechanism. This addition increases the system's ability to provide dynamic and granular authorizations, albeit with a slight performance overhead. However, the average additional cost of this assessment mechanism remains negligible for requesters when compared to attribute-based access control (ABAC).

To evaluate the authorization capabilities of the CARAC model, experiments were conducted by simulating 100 users issuing access requests to the CARAC server. The risk values were evenly distributed across the system's risk range by adjusting the relevant risk factors. As shown in Figure 12, the experiments compared the authorization levels of ABAC and CARAC across different risk scenarios within the system.

Attribute-based access control (ABAC) fails to adjust its authorization levels in response to changes in system risk values, lacking the necessary adaptability to meet evolving risk management requirements. Conversely, the context-aware risk-based access control (CARAC) model offers enhanced flexibility and granularity in authorization through its risk perception capabilities. As system risks escalate, CARAC dynamically reduces au-

thorization levels, enabling flexible user privilege management to prevent the leakage of sensitive information.

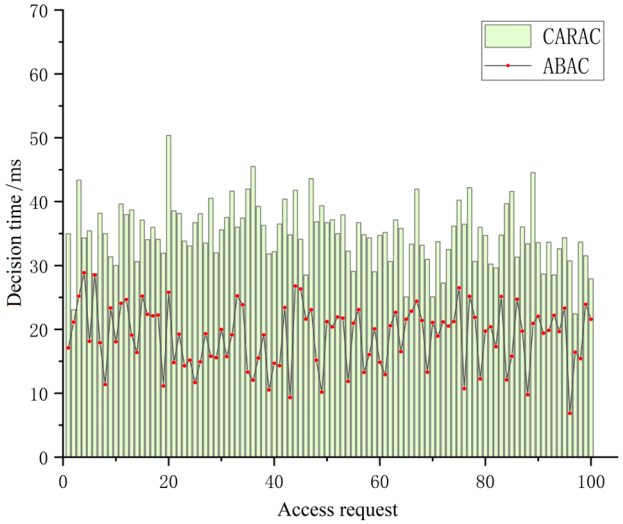

Figure 11. Access control performance analysis.

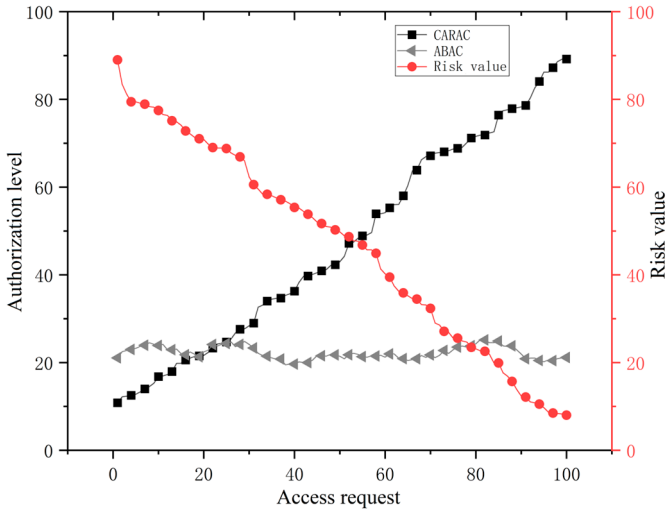

Figure 12. Access control authorization performance analysis.

6. Conclusions

To address the issue of insufficient fine-grained authorization in traditional access control, this study proposes a context-aware risk-based access control model. To accurately evaluate the risk associated with user access, a risk assessment factor system was developed using a combination weighting method from game theory, which integrates both subjective and objective weights. By considering user identity, environmental factors, and behavioral data, the model precisely assesses the risk level of access requests and implements appropriate access control strategies, thereby achieving fine-grained authorization. Experimental results validate the model's usability and its capacity for fine-grained authorization, demonstrating that it can perceive risks during user access and make decisions accordingly, outpacing attribute-based access control (ABAC) in fine-grained authorization while maintaining manageable time costs.

Through this research, access control has broadened its perceptual scope by incorporating context into access strategies, enhancing the model's flexibility, dynamism, and granularity. Future work will focus on improving the accuracy of risk assessments, as this accuracy directly impacts decision-making precision. Although this study employed

game-theoretic combination weighting to ensure weight reasonableness and objectivity to some extent, there remains significant potential for enhancement. Future research could leverage adaptive neuro-fuzzy networks to optimize risk perception, thereby aiming for more accurate risk calculations that better align with real-world scenarios.

Author Contributions: Writing—original draft, S.Z.; Writing—review & editing, B.L. and F.Y. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Sichuan Science and Technology Program, Grant No. 2024NSFSC0515 and No. MZGC20230013.

Data Availability Statement: Data are contained within the article.

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

References

1. Atlam, H.F.; Azad, M.A.; Alassafi, M.O. Risk-based access control model: A systematic literature review. *Future Internet* **2020**, *12*, 103. [CrossRef]
2. Cha, S.C.; Hsuan, Y.H.; Yeh, K.H. An Evolutionary Risk-based Access Control Framework for Enterprise File Systems. In Proceedings of the IEEE 8th World Forum on Internet of Things (WF-IoT), Yokohama, Japan, 26 October–11 November 2022.
3. Ke, C.; Wu, J.; Xiao, F. A privacy risk assessment scheme for fog nodes in access control system. *IEEE Trans. Reliab.* **2021**, *71*, 1513–1526. [CrossRef]
4. Atlam, H.F.; Azad, M.A.; Fadhel, N.F. Efficient NFS model for risk estimation in a risk-based access control model. *Sensors* **2022**, *22*, 2005. [CrossRef] [PubMed]
5. Shaikh, R.A.; Adi, K.; Logrippo, L. Dynamic risk-based decision methods for access control systems. *Comput. Secur.* **2012**, *31*, 447–464. [CrossRef]
6. Yang, H.Y.; Ning, Y.G. A dynamic risk access control model for cloud platform. *J. Xi'an Electron. Sci. Technol. Univ.* **2018**, *45*, 80–88.
7. Ding, H.F.; Peng, C.G. Privacy risk adaptive access control model based on evolutionary game. *J. Commun.* **2019**, *40*, 9–20.
8. Hou, M.W.; Lan, X. Research on the application of privacy protection technology in healthcare big data publishing. *China Digit. Med.* **2020**, *15*, 92–94.
9. Wang, Y.; Jiang, Z.Y. Research on the status quo, problems and countermeasures of information security of healthcare big data in China. *Mod. Med. Health* **2021**, *37*, 3036–3039.
10. Jiang, R.; Yang, X.; Chen, Z. A medical big data access control model based on fuzzy trust prediction and regression analysis. *Appl. Soft Comput.* **2022**, *117*, 108423. [CrossRef]
11. Zhang, W.; Li, H.; Zhang, M. Privacy-aware risk-adaptive access control in health information systems using topic models. In Proceedings of the 23rd ACM on Symposium on Access Control Models and Technologies, Indianapolis, IN, USA, 13–15 June 2018.
12. Jiang, R.; Liu, R.; Zhang, T. An electronic medical record access control model based on intuitionistic fuzzy trust. *Inf. Sci.* **2024**, *658*, 120054. [CrossRef]
13. Wang, J.Y.; Liu, S.R. Research progress on risky access control for big data. *Comput. Sci.* **2020**, *47*, 56–65.
14. Kesarwani, A.; Khilar, P.M. Development of trust based access control models using fuzzy logic in cloud computing. *J. King Saud Univ. Comput. Inf. Sci.* **2022**, *34*, 1958–1967. [CrossRef]
15. Suleiman, D.; Shaout, A. Enhanced Multilevel Fuzzy Inference System for Risk Adaptive Hybrid RFID Access Control System. *Int. J. Online Biomed. Eng.* **2022**, *18*, 31–51. [CrossRef]
16. Zhang, S.W.; Li, B.Y.; Deng, L.M. Adaptive access control model based on context-awareness. *Comput. Appl. Res.* 2024; *in press*.
17. Shi, X.J.; Yu, W.H. A fuzzy neural network based access control risk quantification method. *Intell. Comput. Appl.* **2018**, *8*, 31–35.
18. Oliveira, M.T.; Reis, L.H.A. AC-ABAC: Attribute-based access control for electronic medical records during acute care. *Expert Syst. Appl.* **2023**, *213*, 119271. [CrossRef]
19. Aghili, S.F.; Sedaghat, M. MLS-ABAC: Efficient multi-level security attribute-based access control scheme. *Future Gener. Comput. Syst.* **2022**, *131*, 75–90. [CrossRef]
20. Shao, R.X.; Tian, X.X. ABAC access control scheme based on MQTT protocol in smart grid. *Comput. Appl. Res.* **2022**, *39*, 3436–3443.