applied sciences

MDPI

Article

An Access Control Model Based on System Security Risk for Dynamic Sensitive Data Storage in the Cloud

Nawaf Alharbe [1,*], Abeer Aljohani [1], Mohamed Ali Rakrouki [2,3,4] and Mashael Khayyat [5]

[1] Applied College, Taibah University, Medina 42353, Saudi Arabia
[2] College of Computer Science and Engineering, Taibah University, Medina 42353, Saudi Arabia
[3] Ecole Supérieure des Sciences Economiques et Commerciales de Tunis, University of Tunis, Montfleury 1089, Tunisia
[4] Business Analytics and Decision Making Lab (BADEM) at Tunis Business School, University of Tunis, Bir El Kassaa 2059, Tunisia
[5] Department of Information Systems and Technology, College of Computer Science and Engineering, University of Jeddah, Jeddah 23445, Saudi Arabia
* Correspondence: nrharbe@taibahu.edu.sa

Abstract: In cloud computing, dynamic storage of data generated by users, applications, tasks, workflows, etc. requires frequent access operations, so traditional encryption cannot be applied in this case. Considering the vulnerability of dynamic data, its protection needs to consider an efficient and dynamic security protection scheme. In data-oriented access control, the traditional approach is generally static policy matching, which cannot deal with emergencies and has the problem of privileged users. To solve this problem, this paper proposes a data-oriented risk-based access control model, which adds risk assessment to the traditional attribute-based access control and aims at the source of risk from three aspects: subject attribute, resource attribute, and environment attribute. A set of risk assessment indexes is proposed, and the calculation method of risk assessment is quantitatively analyzed by combining fuzzy consistency AHP analysis method, and finally, the realization of XACML is given. The validity of the proposed model is analyzed, and the carried out experimental analysis verifies its effectiveness. The proposed model benefits cloud data storage applications that require dynamic data storage, for example, medical/patient data storage.

Keywords: computer security; cloud computing; cloud storage; secure medical data storage

check for updates

Citation: Alharbe, N.; Aljohani, A.; Rakrouki, M.A.; Khayyat, M. An Access Control Model Based on System Security Risk for Dynamic Sensitive Data Storage in the Cloud. *Appl. Sci.* **2023**, *13*, 3187. https://doi.org/10.3390/app13053187

Academic Editor: Arcangelo Castiglione

Received: 29 January 2023
Revised: 23 February 2023
Accepted: 28 February 2023
Published: 2 March 2023

Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

Cloud services are increasingly used for storing sensitive data, especially for medical record data storage, data access, and data processing for efficient information gathering. Although challenges exist around data security and integrity as compared to using dedicated, in-house data storage, access, and processing capabilities, the hardware and software resources available within cloud services outweigh any limitations. Patient medical and health data generated by patients, medical professionals, hospitals, applications, devices, tasks, workflows, etc., intended for storage and processing within a cloud service, require frequent access operations to the cloud services due to the dynamic nature of data generation, storage, processing, and access needs. Hence the data vulnerability remains high.

In cloud computing environments, access control is the basic approach used to achieve cloud environment security. Traditional access control mainly comprises an access control model and policy description language. Common access control models are mainly discretionary access control (DAC), mandatory access control (MAC), and role-based access control (RBAC) [1]. These three models are better in a static environment. However, the business environment in cloud computing changes dynamically, especially the security and integrity of the resource access subject environment, and the static rule-based decision-making will bring serious security risks to the system. For example, the traditional

Token-based method is a static access control. After the user passes the identity authentication of the system, the system assigns a Token to the user. Each Token uniquely identifies a user, so in later operations, the system will no longer authenticate the user. The computing environment where the access topic is located typically caches the authentication token to increase authentication efficiency. However, there is a significant security problem with this method. On the one hand, if the security of the main environment deteriorates, the authentication token may be used illegally, resulting in the illegal use of system resources and services; on the other hand, consider a scenario when the system is currently in an emergency state (such as CPU and memory utilization are saturated), traditional access control will continue to accept access requests as long as the request is legitimate, increasing the risk of a system crash.

Through the above analysis, this paper adopts a different strategy, starting from the likelihood that a request could compromise system security, along with the dynamic changes of the object environment, based on attribute-based access control. This paper proposes a set of thorough risk assessment indicators and quantitative analysis models to adapt access control decision-making to the effects of the environment's dynamic change.

The remainder of this paper is organized as follows. A literature review is provided in Section 2. Section 3 introduces the proposed dynamic access model based on risk assessment. Experimental results are provided in Section 4. Finally, the content of this paper is summarized in Section 5.

2. Literature Review

In the cloud environment, the dynamic changes of the user environment add difficulties to resource access control. Risk assessment has been proposed in recent years as an effective solution for dealing with uncertain and difficult-to-control user behaviors in complex environments [2]. This method can evaluate the possibility of users participating in the system behavior and the risks in the user environment to control uncertain user behavior effectively. Therefore, it is very important to study risk assessment for access control.

Dos Santos et al. [3] proposed a dynamic risk-based access control model and introduced three new modules: Risk Engine, Risk Quantification Service, and Risk Policy. Although the research does not disclose precise risk quantification techniques, this approach enables users and cloud service providers to specify how to manage risky access requests. Chen et al. [4] proposed a similar model, with risk measurement serving as a secondary decision indicator. Additionally, a risk threshold is created dynamically from historical data, and the policy, risk assessment, and dynamic threshold all impact the final, holistic choice. To increase its performance, a data stream-based sliding window calculating approach is used. Bijon et al. [5] analyzed the differences between traditional constraint-based risk control and risk quantification methods, proposed an adaptive risk-aware RBAC model, introduced risk in the role-based access control model, and gave a quantitative Risk Analysis Methods. To solve the problem of manual intervention in traditional multi-level security systems, trust and risk values, Shaikh et al. [6] proposed a risk calculation method that can dynamically adapt to historical values, and a dynamic risk access control model is given, and comprehensive decision-making is made through two aspects of trust and risk. Younis et al. [7] provided a comprehensive analysis of cloud computing's access control requirements, identified significant holes that are not addressed by traditional access control approaches, and proposed an access control model to satisfy the defined cloud access control criteria. Namasudra and Roy [8] proposed an innovative access control mechanism for effective data access. The suggested approach retains a popularity score for each large data piece to reduce the number of security issues. The experimental results showed that the suggested strategy resists numerous types of attacks. Recently, ref. [9,10] proposed Blockchain-based access control approaches in cloud computing.

Lin et al. [11] suggests a mutual trust-based access control model that integrates with trust management. This model considers both the trustworthiness of the cloud service provider and user activity. Mutual trust mechanisms are used to build trust between users

and the cloud to resolve access control security issues. Chunge et al. [12] suggests that the concept of trust in role-based access control can help to identify malicious users and ensure the security of the cloud and data. Wu and Liu [13] studied many conventional access control techniques and suggests a hybrid access control technique based on trust in the role-based access control technique. The experiments provided some evidence that the proposed approach can raise the system's trustworthiness, lessen the likelihood that tasks will fail to complete and be spoofed, and stop unauthorized individuals from accessing resources. Satoh [14] proposed a context-aware access control model by integrating role/subject-based models. Only the main concept of the framework and its prototype implementation are presented in this work.

Most of the above studies are aimed at the access control model. In terms of risk quantification, Ni et al. [15] proposed an access control model based on fuzzy reasoning. To realize the risk control based on Binary Linear Programming (BLP), a predefined rule is proposed to decide whether to authorize it by analyzing the authorization risk, but the model does not consider the impact of the user's past behavior on the risk. Cheng et al. [16] proposed a fuzzy multi-level access control model to quantify the risk of access and dynamically control the flow of risk information according to the current system environment, business requirements, and risk tolerance. Li et al. [17] proposed a method based on fuzzy modeling, which takes the sensitivity of data, the risk of doctors' behavior, and historical risk as input and combines historical data and fuzzy sets to calculate the risk level of medical data access. However, this method is aimed at medical data and is not universal. Badar et al. [18] proposed a classification-based approach to risk access control by classifying risk with authorization and combining an access control matrix with role-based access control to assign permissions to the least risky roles. Recently, to quantify the security risk value associated with each access request for diverse IoT applications, Atlam et al. [19] suggested a Neuro-Fuzzy System model. The outcomes of the experiments showed that the suggested approach offers dynamic and contextually aware access decisions based on real-time information. A systematic literature review of dynamic access control models is presented by Atlam et al. [20]. Both the risk assessment approaches and the risk factors that were utilized to construct these are extracted and assessed along with the risks associated with access control procedures. Khan and Mehfuz [21] proposed a fuzzy role-based access control approach by recognizing authentic cloud nodes according to their behavior. The behavioral activity of the node has been examined to obtain the fuzzy maximum periodic values and the volume of transactions has been found proportional to the trustworthiness of the cloud node. Some fuzzy trust-based access control approaches have been proposed by Kesarwani and Khilar [22]. In these approaches, trust values have been calculated based on some criteria, such as faulty requests, fake requests, illegal requests, and the total number of requests.

Beraka and Al-Muhtadi [23] reviewed and examined five reference models of access control in cloud computing. For each model, its components, issues, constraints, and pertinent research have been provided. Some comprehensive surveys on access control models in cloud computing and an in-depth comparison of each model's benefits and drawbacks can be found in [24–29].

3. Risk Assessment-Based Dynamic Access Model

The main scheme of the dynamic access model for risk assessment proposed in this paper is shown in Figure 1.

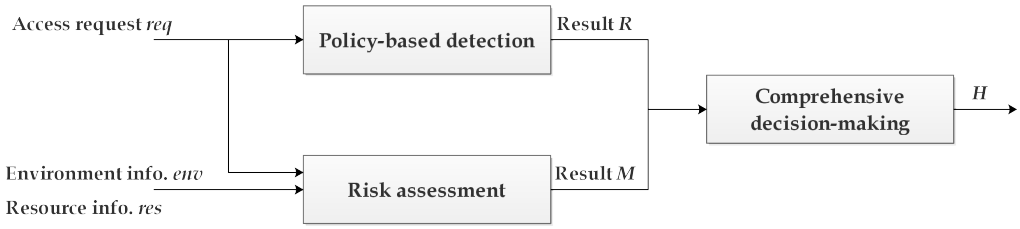

Figure 1. Dynamic Access Control Model Overall Scheme.

This solution mainly includes three core modules: detection based on policy rules, risk assessment of requests, and comprehensive decision-making. The detection module based on policy rules performs static rule-based judgment on the access request *req*, and outputs the result *M*. The request risk assessment calculates the risk assessment value *R* that the current request may pose a threat to the system according to the input object environment information *env*, resource information res, and access request *req*. The comprehensive decision-making module makes the final access control result *H* according to the fusion decision of *R* and *M*. Wherein the object environment information *env* refers to the current environment attributes of the system, and the resource information res refers to the resource status requested to be accessed.

3.1. Request a Risk Assessment

Traditional static control strategies may face an embarrassing situation: as time changes, the judgment rules for requests in the past may be incorrect at this moment. The realization of dynamic security control is the most important link in this model.

3.1.1. Establishment of Risk Assessment Indicators for Access Requests

Since risk is an abstract and dynamic concept, to assess risk better and reflect real scenarios, this paper divides risk assessment into three layers, namely the target layer, attribute layer, and the evidence layer, and refines the three attributes layer by layer into the evidence values that the system can directly obtain in the process of requesting access.

The target layer is the target we evaluate risk. In terms of the division of the attribute layer, because this paper mainly evaluates the risk that the access may cause to the system, the attribute layer is divided into three main aspects according to the source of the risk: main attribute, resource attribute, and environmental attribute. Below we will analyze in detail the selection of indicators from three aspects: subject, resource, and environment.

In terms of subject attributes, the subject here is mainly the initiator of the request, mainly referring to the user, but not limited to the user, but also an application, a virtual machine or a workflow, and so on. The request is the process of the subject requesting the system to operate a certain resource, so the request is embodied as the subject's behavior in the system. On the one hand, the behavior is the specific operation of the subject on the resource request, such as reading, writing, or copying a resource request. These operations have different sensitivity levels. From the perspective of possible risks to the system, the sensitivity level of writing is the highest; On the other hand, the historical preference behavior of the subject is mainly reflected in the common time of the subject initiating the request, the common IP, the historical request success rate, the number of historical login failures, etc. The system maintains the behavior history of each subject for the current request risk assessment. For example, when a subject fails to log in multiple times, the system will determine that the request is a potential attack and has high risk, so it will ask for a verification code when logging in next time; and a subject initiates a written request to the resource. The system query finds that if the historical success rate of the subject's request to write to the resource is high, the subject will accept the request because the risk of this request is low.

Regarding resource attributes, resources mainly refer to data in this article. Access control's primary goal is to prevent unauthorized access to system resources. However, data security will also be somewhat impacted by how vulnerable the data is. Here we define

the vulnerability of data to refer to various security risks in the data itself or the protection methods of the data. Attackers can relatively easily destroy, obtain, and tamper with the data by exploiting such security risks. First of all, the storage method of data resources is also one of the factors affecting the vulnerability of resources. When data are encrypted and stored in the system, if the decryption key is unavailable, even if the adversary obtains the encrypted data, there is no way to decrypt it. Secondly, the importance of data is also a factor that affects the vulnerability of resources. If the importance of data is high, the risk of accessing requests to operate on it will also increase.

In terms of environmental attributes, this paper divides the environmental attributes into two aspects, namely, the environment of the terminal and the environment of the server. The terminal environment is mainly used to measure the security of the user terminal, such as the IP packet loss rate. If the current IP packet loss rate is high, it means that the network connection where the user is located is unstable, which not only reduces the quality of service but also brings viruses to resources. Or the risk of attack; the current environment of the server will also affect the risk of access requests; for example, the current CPU or I/O consumption of the server is saturated. There is a risk of node paralysis.

Through the above analysis, we refined the risk evidence layer and established the request risk evaluation index, as shown in Figure 2.

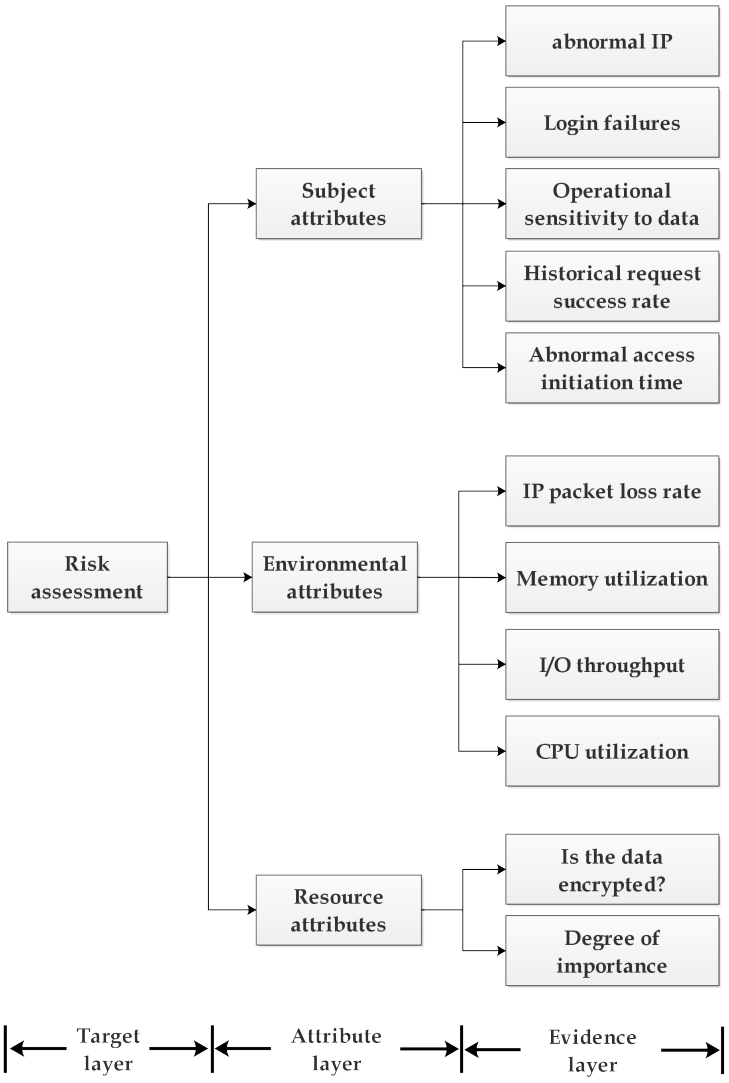

Figure 2. Access Request Risk Assessment Metrics.

3.1.2. Calculation and Standardization of Attribute Evidence

How to obtain evidence of the above properties is the basis of risk assessment. For the subject attribute, you can obtain it by accessing the request itself and the system history. For the environment attribute, you can obtain it through system monitoring. The resource attribute can be obtained through the system storage system log. It should be noted that the sensitivity of data operations is measured. Since different operations have different levels of risk, we define AS as the security sensitivity of operation A. The operation's impact on system security increases with operation sensitivity. By running a query against the appropriate security sensitivity table, one can determine the security sensitivity of various actions. For instance, read, write, copy, and execute have security sensitivities of 0.2, 0.4, 0.6, and 0.8, respectively.

To make the calculation of attribute evidence more objective, in the main attributes, the IP anomaly, the number of login failures, the historical request success rate, and the abnormal access initiation time will decay with time; that is, the longer the distance from the current time. The greater the value, the greater the impact on the request risk, which means that if the user performs more abnormal operations in a short period of time, the request is abnormal, and the possibility of damaging the security behavior of the system is greater, and the risk value is also high. This paper uses Equation (1) to calculate the four evidence values of IP anomaly, login failure, historical request success rate, and abnormal access initiation time:

$$S_{new} = \begin{cases} S_{old} \cdot [1 + \varphi(\Delta S)]; & t < t_0 \\ S_{old} \cdot \phi(t); & t > t_0 \end{cases} \quad (1)$$

Among them, S_{new} represents the updated value of the evidence, S_{old} represents the value before the update, t_0 represents the valid time of the evidence value, and $\phi(t)$ is the time decay function. When $t > t_0$, it indicates that the evidence value is within this time interval. If there is no update, the evidence value is processed according to the time decay; when the time interval t is less than t_0, it means that the new evidence value is obtained within the valid time, but the new evidence value cannot completely replace the old evidence value, so the use between the two is used. The increment $\Delta S = S_{new} - S_{old}$ to update the evidence, $\varphi(\Delta S)$ is the increment control function.

In addition, since each piece of evidence has different meanings and different value ranges, it is necessary to standardize the data so that the values fall within the range of $[0, 1]$. For the evidence that the value is a percentage, its value is already in the range of $[0, 1]$, so it can be represented by a decimal, such as the IP packet loss rate, memory utilization, CPU utilization, etc. in the environment attribute; in addition, for the resource attribute Whether the data in is encrypted, its value is only two, namely 0 or 1, and no processing is required. The value of operation sensitivity is given in Table 1, and no processing is required; for other evidence, it is assumed that the obtained evidence of an attribute is $A = (a_1, a_2, ..., a_n)$, and the attribute evidence after standardized processing is $E = (e_1, e_2, ..., e_n)$, then the specific data standardization processing is as Equation (2).

Table 1. Operational Security Sensitivity [4].

	$Attr(a)$	AS
1	Read	0.2
2	Copy	0.4
3	Write	0.6
4	Execute	0.8

$$e_i = \begin{cases} \dfrac{a_i - \min(a_i)}{\max(a_i) - \min(a_i)}; & a_i > 0 \\ \dfrac{\max(a_i) - a_i}{\max(a_i) - \min(a_i)}; & a_i < 0 \end{cases} \quad (2)$$

In the above way, all evidence values can be converted into positive values between $[0, 1]$.

3.1.3. Indicator Weight Calculation

The accuracy of the evaluation results depends on the scientificity and rationality of the index weights. The traditional method for establishing indicator weights is to assign initial values based on experience and then continuously revise them according to the actual situation. However, due to the variability and uncertainty of the actual situation, this method is not only time-consuming but also the results obtained are not necessarily accurate. For this reason, this paper adopts the analytic hierarchy process in the multi-attribute decision-making related theory to assign the weights of the indicators. In the scenario of this paper, due to the correlation between the various attribute evidence in the risk analysis, this paper introduces the Fuzzy Analytic Hierarchy Process (FAHP) [30] to quantify the risk of the access request so as to construct an integrated multivariate access request security risk assessment model. This method not only reduces the subjective impact of its process but also takes into account the correlation of risk factors, making the assessment more objective and credible.

FAHP is an improvement to the Analytic Hierarchy Process (AHP) [31], which solves the problem of repeatedly adjusting and testing the judgment matrix in the consistency test of the traditional AHP. This method first divides the target into n attributes. Then, these attributes are divided into several detailed pieces of evidence, which are the direct reflection of the attributes, thereby simplifying the dynamics and uncertainty of cloud computing user behavior. Corresponding to this paper, the risk objectives are divided into main attributes, resource attributes, and environmental attributes. Each attribute is further divided into several pieces of evidence that can be obtained by the system. The related FAHP concepts are briefly explained in the following.

Definition 1. *The fuzzy matrix A is defined as $A = (a_{ij})_{n\times n}, \Omega = \{1, 2, ..., n\}$, if there is $0 \le a_{ij} \le 1 (i, j \in \Omega)$.*

Definition 2. *The fuzzy complementary matrix is defined as $A = (a_{ij})_{n\times n}, \Omega = \{1, 2, ..., n\}$, if there is $a_{ij} + a_{ji} = 1; \forall i, j \in \Omega$.*

Definition 3. *The fuzzy consistency matrix is defined as $A = (a_{ij})_{n\times n}, \Omega = \{1, 2, ..., n\}$, if there is $a_{ij} = a_{ik} - a_{jk} + 0.5; \forall i, j \in \Omega$.*

Theorem 1. *The matrix $R = (r_{ij})_{n\times n}$ obtained by converting the fuzzy complementary matrix A according to Equations (3) and (4) must also be fuzzy.*

$$r_i = \sum_{k=1}^{n} a_{ik}, i = \{1, 2, ..., n\} \quad (3)$$

$$r_{ij} = \frac{r_i - r_j}{2(n-1)} + 0.5 \quad (4)$$

Assuming that in the risk assessment index, the attribute layer element groups are $\{B_1, B_2, ..., B_n\}$, and there are evidence layer elements $\{B_{i1}, B_{i2}, ..., B_{in}\}$ in the attribute B_i, and n is the number of evidence layer elements in the attribute B_i, taking the risk T as the target, compare the influence degree of the attribute layer and evidence layer elements on the target. Based on the influence degree of each attribute on risk, this paper uses the "1∼9 value" method of Saaty [30] to determine the importance ratio of two elements. Saaty

proved the rationality of the "1∼9" scale with a large number of experiments, and the "1∼9 value" method has been recognized and widely used. The scale meanings are shown in Table 2.

Table 2. Scale values.

Scale	Meaning
1	The former is extremely less important than the latter
3	The former is slightly less important than the latter
5	Two factors are of equal importance compared to each other
7	The former is significantly more crucial than the latter
9	The former is far more crucial than the latter.
2, 4, 6, 8	indicate the midpoints between the aforementioned neighboring judgments.

(1) Evidence Layer—Attribute Layer:

According to Table 2, construct the initial judgment matrix EQ of the evidence layer:

$$EQ = \begin{Bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{Bmatrix}$$

Then the initial judgment matrix EQ is transformed into the fuzzy consistency matrix Q according to Equations (3) and (4):

$$Q = \begin{Bmatrix} r_{11} & r_{12} & \dots & r_{1n} \\ r_{21} & r_{22} & \dots & r_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ r_{n1} & r_{n2} & \dots & r_{nn} \end{Bmatrix}$$

Calculate the weight vector W_{C_i} of n evidences in attribute C_i:

$$W_{C_i} = \{w_{C_1}, w_{C_2}, ..., w_{C_n}\}^T \tag{5}$$

where w_i is:

$$w_{C_i} = \frac{\sum_{j=1}^{n} a_{ij}}{\sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}} \tag{6}$$

(2) Attribute Layer—Target Layer:

Similarly, first, calculate the attribute layer to determine the initial matrix EQ'.

$$EQ' = \begin{Bmatrix} b_{11} & b_{12} & \dots & b_{1n} \\ b_{21} & b_{22} & \dots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \dots & b_{nn} \end{Bmatrix}$$

Then the initial judgment matrix EQ is transformed into a fuzzy consistency matrix Q' according to Equations (3) and (4), and then the weight vector W of each attribute B_i of risk is calculated:

$$W = \{w_1, w_2, ..., w_n\}^T \tag{7}$$

(3) Risk calculation:

From Equations (5) and (7), the value of risk R can be obtained:

$$R = W_{C_i} \cdot W^T \tag{8}$$

Compare the calculated risk value with the membership degrees of risk levels in Table 3, judge the risk level, and make a decision to allow or deny the request according to the specific situation of the system.

Table 3. Request risk membership level.

Level	Risk Description
$0.8 < R \leq 1.0$	Extreme risk level, data resources are very insecure
$0.6 < R \leq 0.8$	High-risk level, data resources are very insecure
$0.4 < R \leq 0.6$	At risk, data resources are very insecure
$0.2 < R \leq 0.4$	The risk level is lower, data resources are more secure
$0.0 < R \leq 0.2$	Low risk level, safe data resources

3.1.4. Risk Assessment Process

According to the analysis in the previous section, taking the degree of impact on the risk as the standard, first, calculate the weights of the three attributes of the risk: the main attribute B_1, the environmental attribute B_2 and the resource attribute B_3, which are obtained by comparing the importance of each pair, as shown in Table 4.

Table 4. Attribute pairwise comparison result.

Risk	C_1	C_2	C_3	$\sum C_i$
C_1	0.5	0.7	0.8	2
C_2	0.3	0.5	0.6	1.4
C_3	0.2	0.4	0.5	1.1

We obtain the attribute initial judgment matrix EQ according to Table 4:

$$EQ = \begin{Bmatrix} 0.5 & 0.7 & 0.8 \\ 0.3 & 0.5 & 0.6 \\ 0.2 & 0.4 & 0.5 \end{Bmatrix}$$

The fuzzy matrix Q of the matrix EQ is calculated according to Equation (4):

$$Q = \begin{Bmatrix} 0.5 & 0.65 & 0.725 \\ 0.35 & 0.5 & 0.575 \\ 0.275 & 0.425 & 0.5 \end{Bmatrix}$$

The weight vector of the attribute layer of risk calculated by Equation (6) is $W = \{0.396, 0.321, 0.283\}^T$. The weight vector of the evidence layer is calculated below. Taking the subject attribute as an example, the important relationship between the pieces of evidence is compared in pairs as shown in Table 5.

Table 5. Pairwise comparison results of subject attribute evidence.

	D_1	D_2	D_3	D_4	D_5
D_1	0.5	0.4	0.5	0.3	0.6
D_2	0.6	0.5	0.6	0.4	0.7
D_3	0.5	0.4	0.5	0.3	0.6
D_4	0.7	0.6	0.7	0.5	0.9
D_5	0.4	0.3	0.7	0.1	0.5

Similarly, according to Equations (3) and (4), the fuzzy matrix of the subject attribute evidence is obtained as

$$Q_{C_1} = \begin{Bmatrix} 0.5 & 0.4375 & 0.5 & 0.3625 & 0.575 \\ 0.5625 & 0.5 & 0.5625 & 0.425 & 0.6375 \\ 0.5 & 0.4375 & 0.5 & 0.3625 & 0.65 \\ 0.6375 & 0.65 & 0.6375 & 0.5 & 0.7125 \\ 0.425 & 0.3625 & 0.425 & 0.575 & 0.5 \end{Bmatrix}$$

The weight vector of the subject attribute evidence calculated by Equation (6) is $W_{C_1} = \{0.202, 0.185, 0.202, 0.172, 0.239\}^T$. Similarly, the weight vectors for computing resource attributes and environmental attributes are $W_{C_2} = \{0.255, 0.280, 0.225, 0.240\}^T$ and $W_{C_3} = \{0.486, 0.5139\}^T$. Finally, the value obtained by the system is calculated by Equation (8) and combined with the weight value to obtain the risk value.

3.2. Policy Rule Checking

In the dynamic access control model, the static processing of access requests is a set of access control based on policy rules. The rules use attributes for rule detection. Attributes are physical quantities used to describe the inherent characteristics of entities. Attributes can be divided into subject attributes and objects. There are three types of attributes and environmental attributes. The operation of attributes is also a part of rule detection. The specific definitions are as follows:

1. Four elements V, X, Y, Z, representing the subject set, the object set, the environment set, and the operation set, respectively.
2. Subject attribute VA, object attribute XA, resource attribute YA and operational attribute ZA, where

$$VA_k(1 \le k \le K)$$
$$XA_m(1 \le m \le M)$$
$$YA_j(1 \le j \le J)$$
$$ZA_n(1 \le n \le N)$$

3. The attribute assignment relationship of the corresponding instances V, X, Y, and Z:

$$Attr(V) \subseteq \{VA_1 \times VA_2 \times ... \times VA_k\}$$
$$Attr(X) \subseteq \{XA_1 \times XA_2 \times ... \times XA_M\}$$
$$Attr(Y) \subseteq \{YA_1 \times YA_2 \times ... \times YA_J\}$$
$$Attr(Z) \subseteq \{ZA_1 \times ZA_2 \times ... \times ZA_N\}$$

4. In policy rule ABAC, policy z is specified as $\{sign \leftarrow (Attr(V), Attr(X), Attr(Y), Attr(Z))\}$, sign indicates authorization (0 or 1). There could be several policies that a request matches. Equation (9) illustrates how the security policy library's policy rules impact the outcome of the present request *req*.

$$M(z_j) = z_1 \bigcap z_2 \bigcap z_3 \bigcap ... \tag{9}$$

3.3. Comprehensive Decision-Making

In the comprehensive decision-making of risk assessment and policy rule detection, the results of policy rule detection are mainly used, and risk assessment is supplemented to make decisions on requests. Mainly divided into the following situations:

1. When the detection result of the policy rule is *deny*, the request is rejected regardless of the risk assessment result, that is, the comprehensive decision H is *deny*.
2. When the policy rule detection result is *allow*, the decision is based on the risk assessment result: when the requested risk assessment value is $[0.0, ..., 0.4]$, it indicates that the request risk value is low, the system resources are in a safe state, and the com-

prehensive decision is *allow*; When the risk assessment value of the request is greater than 0.8, it means that the request risk is very high, and the comprehensive decision is *deny*; when the risk assessment value of the request is $[0.4, ..., 0.8]$, it means that the request risk value is high and the system resources are in a relatively unsafe state. The configuration determines whether the decision result is *deny* or *allow*. For example, if the administrator sets a low-risk tolerance of the system, the comprehensive decision is *deny*, and if the risk tolerance is high, *allow*.

3.4. Implementation of The Proposed Model on XACML

Based on eXtensible Access Control Markup Language (XACML), this paper implements the proposed dynamic access control model. As shown in Figure 3, the model is based on Policy Information Point (PIP), Policy Decision Point (PDP), and Policy Enforcement Point (PEP). PIP is responsible for encapsulating the attribute information of the request *req*, and PDP is used for decision-making. The specific process is as follows:

1. The user makes an access request $req\{V, X, Y\}$, where V, X, Y represent the subject, the action, and the resource, respectively;
2. The PEP submits the user request *req* to the PIP through the XACML context syntax;
3. PIP queries the relevant attribute engine to obtain the context attribute information of the current *req* (IP address, MAC address, time, etc.);
4. The attribute engine returns the property value of *req*;
5. PIP adds the context attribute value to the *req* request and passes it to the PEP through the XACML context;
6. PEP submits the reconstructed $req\{V, X, Y, Z\}$ to the policy rule detection module and risk monitoring module of the PDP;
7. The policy rule detection module performs static rule judgment on the request according to the policy rule and obtains the judgment result $M(z_j)$. The risk assessment module adopts the method proposed in Section 3.1 to evaluate the risk of the access request and obtains the risk assessment result $R(req_i)$;
8. The risk assessment detection result and the policy rule detection result are submitted to the comprehensive assessment module, which performs a comprehensive assessment of the risk assessment result and the rule assessment result, and gives the comprehensive assessment result $H(req_i)$;
9. The decision module determines whether the decision for the current request *req* is *allow* or *deny* according to the value of $H(req_i)$.

Under the above framework, when a cloud user makes an access request to a resource, it needs to go through the above 9 steps. While the request is judged by the policy rules, the environment of the requesting subject must pass the risk assessment. Moreover, the risk assessment algorithm in this model adopts the detection strategy of fuzzy AHP, which has less resource overhead and more accurate assessment results. Therefore, compared with the traditional access control model and other security models with risk detection, this framework can more accurately assess risks and protect the security of cloud resources.

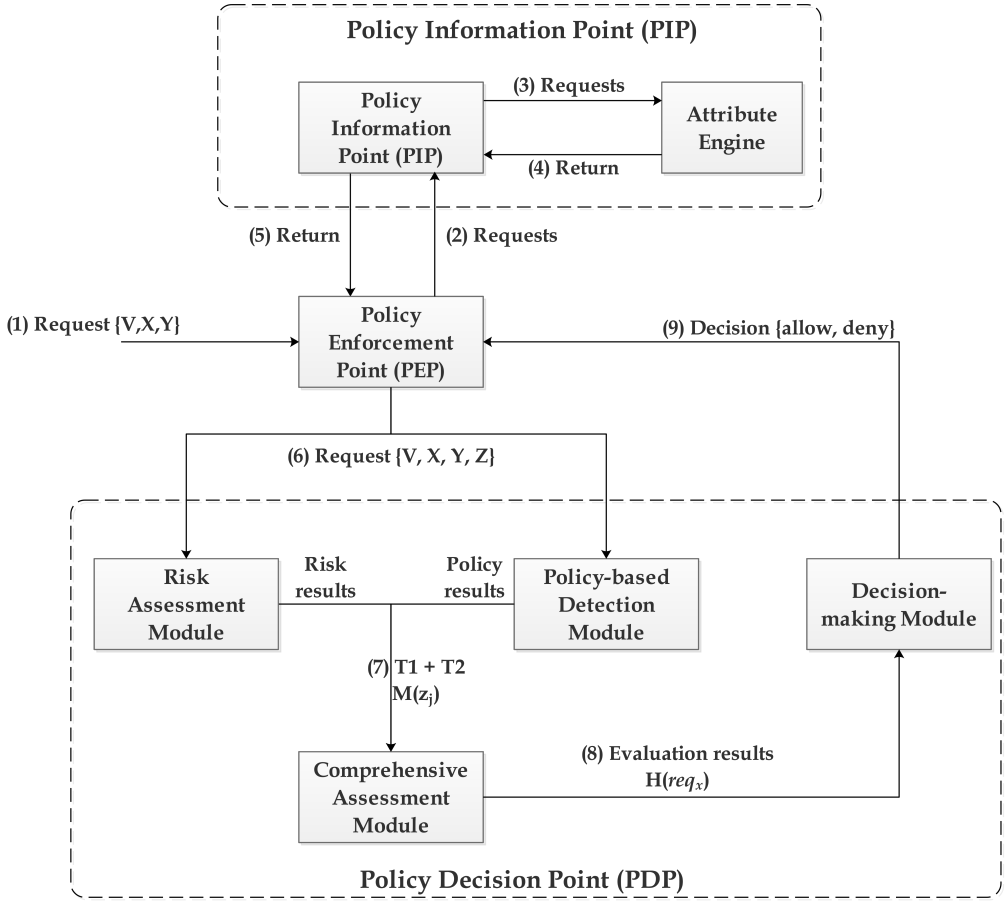

Figure 3. Risk access control model based on XACML.

4. Experimental Results

4.1. Experimental Environment

To simulate the experimental environment, we set up two virtual machines M_1 and M_2 on the OpenStack platform to simulate two web servers. The virtual machines provide web services through Tomcat. The virtual machine M_1 deploys the traditional token-based access control, and the risk access control model proposed in this paper is deployed in the virtual machine M_2. Furthermore, the open-source monitoring software Nagios is installed in the system to keep track of the network and system running status to monitor the virtual machines properly. The hardware configuration of the two virtual machines is the same: quad-core processor, 3.20 GHz, 8 GB memory, 100 Mbps bandwidth, Ubuntu 12.04 64-bit system.

The experiment constructed a large number of normal requests and set it up to send 100 requests per second to two virtual machines simultaneously. During the experiment, the firewall of the virtual machine was turned off to allow the attack to succeed. Nagios collects data about the current environment every 2 min and writes it to the log.

4.2. Experimental Results and Analysis

First of all, this paper tests the impact of environmental attributes on risk assessment. For virtual machine M_2, we constructed a large number of normal requests. The experiment is set to send 100 requests per second, operate the virtual machine at 500 s, and manually start 5 computation processes, which consume CPU resources to test the relationship between system CPU consumption and risk assessment. We sample the test results. The CPU monitoring data comes from Nagios. The test results are shown in Figure 4.

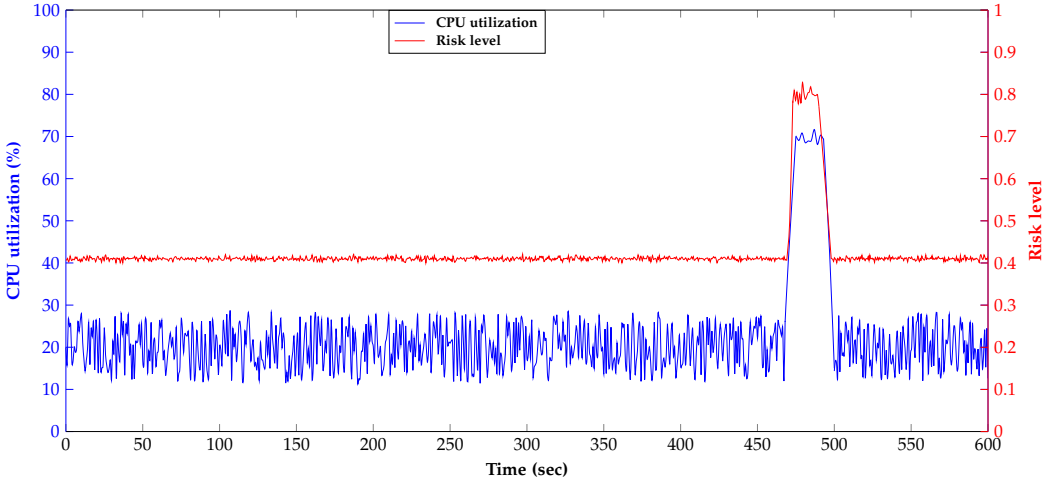

Figure 4. The relationship between the risk value and CPU utilization of virtual machine M_2.

From Figure 4, we can see that the normal range of CPU consumption of virtual machine M_2 is between 15% and 30%, and the normal value of risk assessment is 0.4; that is, the risk level is low. The CPU consumption of virtual machine M_2 increases to 75% at 500 s, and the corresponding risk assessment value also increases to 0.85. The system is in a state of high-risk level and extremely insecure resources, indicating that the risk assessment algorithm proposed in this paper can accurately assesses risks and reflects the real situation.

In the second experiment, we increased the network packet loss rate, combined with CPU utilization, to comprehensively test the impact on the risk value. We set the network packet loss rate in the virtual machine network card. The result is shown in Figure 5. From the figure, we can see that the risk value fluctuates with the fluctuation of CPU utilization and the rate of network packet loss and can respond quickly to them. This is because the proposed quantization method can be calculated in polynomial time, and the proportion of network bandwidth occupied by the transmission of the results is small, so the risk assessment model proposed in this paper is efficient.

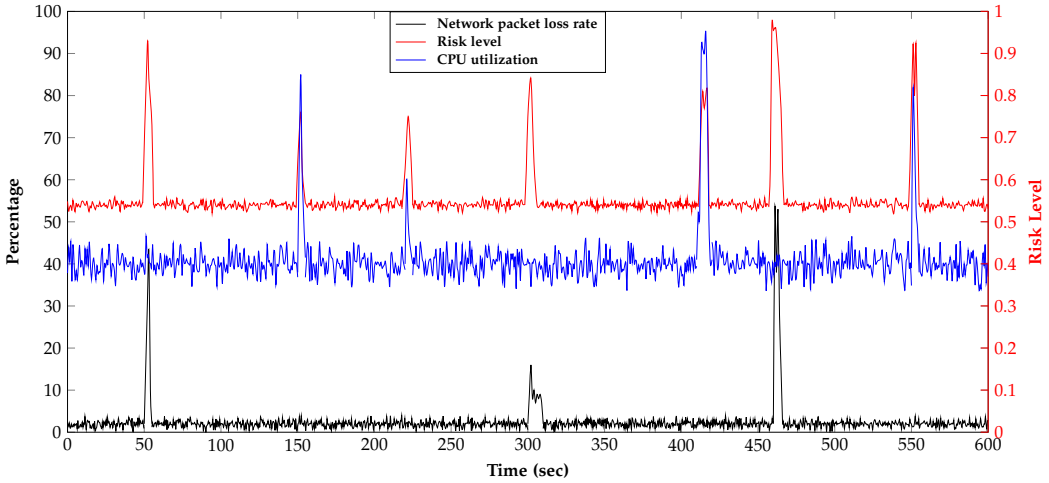

Figure 5. The relationship between the risk value of virtual machine M_2 and the attack.

Next, we conduct a third experiment to test the percentage of rejected requests and the response time of the virtual machines M_1 and M_2 in the presence of abnormal requests. The experiment is also set to 100 requests per second. At the 100th second, virtual machines M_1 and M_2 are operated, and 5 computing processes are manually started to make the CPU resource consumption reach 60%. At the 300th second, 10 calculations are started.

process, so that the CPU resource consumption of the two virtual machines reaches 90%, and an unauthorized access request is added at the 500th second. The resulting percentage of rejected requests is shown in Figure 6.

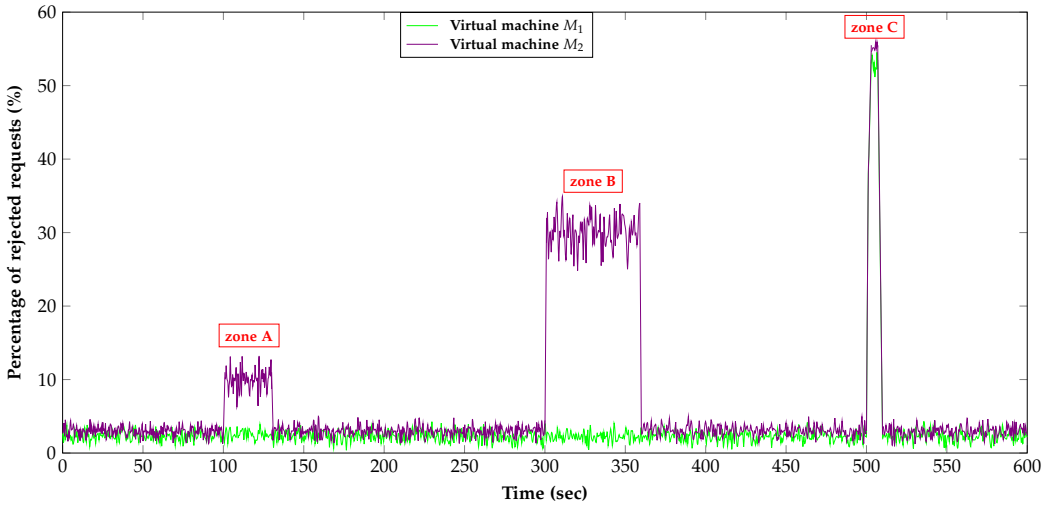

Figure 6. Comparison of request interception rates of the virtual machines M_1 and M_2.

As can be seen from Figure 6, between 0 and 300 s, the percentage of rejected requests of the virtual machines M_1 and M_2 is not much different, almost coincident, and most requests can be processed normally, and the access success ratio is maintained at above 95. At the 100th second, which is zone A in Figure 6, the CPU utilization of both virtual machines reaches 60%, and the percentage ratio of rejected requests of virtual machine M_1 rises to 13%. From the first experiment, we can get this because the high CPU utilization affects the risk assessment value of the request, so virtual machine M_2 will reject some requests with high-risk value, and ordinary access control will not reject legitimate access requests because it does not consider the current system environment, so the percentage of rejected requests for M_1 remains unchanged.

At the 300th second, that is, zone B in Figure 6, the CPU utilization of both virtual machines reaches 90%. Because ordinary access control will receive and process requests as long as the requests are legal, the rejection ratio of virtual machine M_1 is maintained unchanged, but the percentage of rejected requests of virtual machine M_2 has risen to 34%. This is because a risk assessment has been added to the virtual machine M_2. When the system environment is abnormal, such as abnormally high CPU utilization, the requested risk assessment value will increase. To protect the system and resource security, virtual machine M_2 will reject requests with high-risk values. At the 500th second (zone C in Figure 6), illegal requests are added, and both access controls can detect illegal requests, so the rejection percentages go up.

Figure 7 shows the response times of M_1 and M_2 at the 300th second.

In Figure 7, because virtual machine M_1 continues to receive and respond to requests, it continuously occupies already tense resources and increases the system burden. Therefore, the request-response time is about 1100 ms for a long time. In the local area network, this delay is unbearable, and to protect the security of the system, virtual machine M_2 rejected the request with a high-risk assessment value, which guaranteed the response time and prevented the system from facing the risk of crashing due to continuing to receive requests, although this would cause a certain degree of misjudgment. However, compared with the losses caused by system crashes, it is acceptable to sacrifice a certain accuracy rate to ensure that the system and resources are always in a relatively safe state and avoid causing greater losses. In the recovery phase, since the risk assessment of virtual machine M_2 protects the system resources from being overused, it can recover from the anomaly faster than virtual machine M_1.

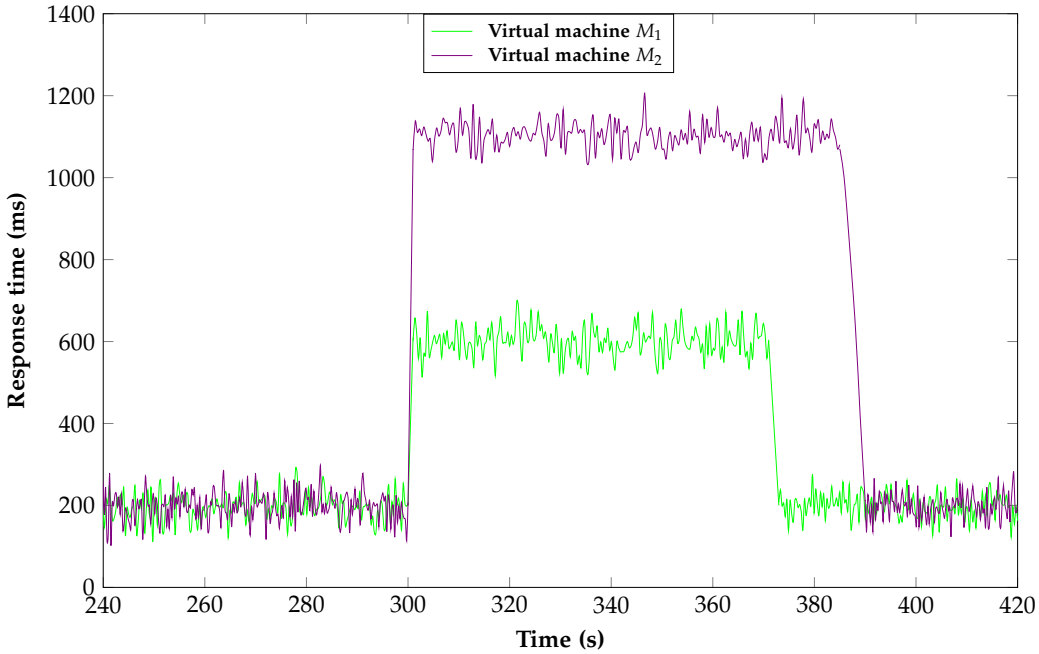

Figure 7. The response times of virtual machines M_1 and M_2 at 300 s.

Through the above experiments, we can see that the risk-based access control strategy proposed in this paper can perform a risk assessment on requests according to the dynamic changes of subjects, resources, and environments and make corresponding decisions, which dynamically protects the system and resources from a relatively secure state, to avoid system crash and cause greater losses. The evaluation method is simple and efficient and has great feasibility. The proposed access control method is ideal for ensuring the security of cloud-based dynamic medical data storage, processing, and access.

5. Conclusions

This paper presents a novel dynamic access control strategy suitable for a wide range of cloud-based application scenarios, for example, secure storage, processing, and access to medical/patient data. A set of risk assessment indicators are derived from subject, resource, and environment attributes, according to the characteristics of the access request, and based on fuzzy consistency. The fuzzy AHP method adopted provides a specific method of calculating the weight and then gives the realization of the access control policy based on XACML. Finally, experiments have been used to verify the effectiveness of the model.

The access control model proposed in this paper has certain limitations, which need to be further improved and perfected. Future research work will mainly focus on the following two aspects:

- In risk-based access control, the selection of risk judgment indicators is not perfect, and the judgment of subjects and resources and the experimental part need to be further improved.
- With the advent of the era of big data, how to ensure the storage security of massive data is a direction worth studying.

Author Contributions: Conceptualization, N.A. and M.A.R.; methodology, N.A. and A.A.; validation, N.A., M.A.R. and M.K.; formal analysis, N.A. and M.A.R. and A.A.; investigation, A.A. and M.K.; resources, N.A., A.A. and M.K.; data curation, N.A., A.A., M.A.R. and M.K.; writing—original draft preparation, N.A. and M.A.R.; writing—review and editing, N.A. and A.A.; visualization, N.A., A.A. and M.A.R. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data used and analyzed during the current study are available from the corresponding author on reasonable request.

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

References

1. Atlam, H.F.; Alenezi, A.; Walters, R.J.; Wills, G.B. An overview of risk estimation techniques in risk-based access control for the internet of things. In Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security, Porto, Portugal, 24–26 April 2017; pp. 254–260. [CrossRef]
2. Bezzateev, S.V.; Elina, T.N.; Mylnikov, V.A.; Livshitz, I.I. Risk assessment methodology for information systems, based on the user behavior and it-security incidents analysis. *Sci. Tech. J. Inf. Technol. Mech. Opt.* **2021**, *21*, 553–561. [CrossRef]
3. Santos, D.R.D.; Westphall, C.M.; Westphall, C.B. A dynamic risk-based access control architecture for cloud computing. In Proceedings of the IEEE/IFIP NOMS 2014—IEEE/IFIP Network Operations and Management Symposium: Management in a Software Defined World, Krakow, Poland, 5–9 May 2014. [CrossRef]
4. Chen, A.; Xing, H.; She, K.; Duan, G. A Dynamic Risk-Based Access Control Model for Cloud Computing. In Proceedings of the 2016 IEEE International Conferences on Big Data and Cloud Computing (BDCloud), Social Computing and Networking (SocialCom), Sustainable Computing and Communications (SustainCom) (BDCloud-SocialCom-SustainCom), Atlanta, GA, USA, 8–10 October 2016; pp. 579–584. [CrossRef]
5. Bijon, K.Z.; Krishnan, R.; Sandhu, R. A framework for risk-aware role based access control. In Proceedings of the 2013 IEEE Conference on Communications and Network Security, CNS, National Harbor, MD, USA, 14–16 October 2013; pp. 462–469. [CrossRef]
6. Shaikh, R.A.; Adi, K.; Logrippo, L. Dynamic risk-based decision methods for access control systems. *Comput. Secur.* **2012**, *31*, 447–464. [CrossRef]
7. Younis, Y.A.; Kifayat, K.; Merabti, M. An access control model for cloud computing. *J. Inf. Secur. Appl.* **2014**, *19*, 45–60. [CrossRef]
8. Namasudra, S.; Roy, P. PpBAC: Popularity based access control model for cloud computing. *J. Organ. End User Comput.* **2018**, *30*, 14–31. [CrossRef]
9. Sabzmakan, A.; Mirtaheri, S.L. An Improved Distributed Access Control Model in Cloud Computing by Blockchain. In Proceedings of the 26th International Computer Conference, Computer Society of Iran, CSICC, Tehran, Iran, 3–4 March 2021. [CrossRef]
10. Yang, C.; Tan, L.; Shi, N.; Xu, B.; Cao, Y.; Yu, K. AuthPrivacyChain: A Blockchain-Based Access Control Framework with Privacy Protection in Cloud. *IEEE Access* **2020**, *8*, 70604–70615. [CrossRef]
11. Lin, G.; Wang, D.; Bie, Y.; Lei, M. MTBAC: A mutual trust based access control model in Cloud computing. *China Commun.* **2014**, *11*, 154–162. [CrossRef]
12. Chunge, L.; Mingji, M.; Bingxu, L.; Shuxin, C. Design and Implementation of Trust-based Access Control Model for Cloud Computing. In Proceedings of the IEEE Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), Chongqing, China, 12–14 March 2021; pp. 1934–1938. [CrossRef]
13. Wu, Y.; Liu, P. Research on Trust-Role Access Control Model in Cloud Computing. *Int. J. Adv. Netw. Monit. Control.* **2019**, *4*, 75–80. [CrossRef]
14. Satoh, I. Context-aware access control model for services provided from cloud computing. *Stud. Comput. Intell.* **2017**, *737*, 285–295. [CrossRef]
15. Ni, Q.; Bertino, E.; Lobo, J. Risk-based access control systems built on fuzzy inferences. In Proceedings of the 5th International Symposium on Information, Computer and Communications Security, ASIACCS 2010, New York, NY, USA, 13 April 2010; pp. 250–260. [CrossRef]
16. Cheng, P.C.; Rohatgi, P.; Keser, C.; Karger, P.A.; Wagner, G.M.; Reninger, A.S. Fuzzy Multi-Level Security: An experiment on quantified risk-adaptive access control. In Proceedings of the IEEE Symposium on Security and Privacy, Berkeley, CA, USA, 20–23 May 2007; pp. 222–227. [CrossRef]
17. Li, J.; Bai, Y.; Zaman, N. A fuzzy modeling approach for risk-based access control in eHealth cloud. In Proceedings of the 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, Melbourne, VIC, Australia, 16–18 July 2013; pp. 17–23. [CrossRef]
18. Badar, N.; Vaidya, J.; Atluri, V.; Shafiq, B. Risk Based Access Control Using Classification. In *Automated Security Management*; Al-Shaer, E., Ou, X., Xie, G., Eds.; Springer International Publishing: Cham, Switzeland, 2013; pp. 79–95. [CrossRef]
19. 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]
20. Atlam, H.F.; Azad, M.A.; Alassafi, M.O.; Alshdadi, A.A.; Alenezi, A. Risk-based access control model: A systematic literature review. *Future Internet* **2020**, *12*, 103. [CrossRef]
21. Khan, A.J.; Mehfuz, S. Secure access control model for cloud computing environment with fuzzy max interval trust values. *Int. J. Adv. Comput. Sci. Appl.* **2020**, *11*, 536–542. [CrossRef]

22. 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]
23. Beraka, M.; Al-Muhtadi, J. Critical comparison of access control models for cloud computing. *J. Internet Technol.* **2015**, *16*, 431–442. [CrossRef]
24. Almutairi, S.; Alghanmi, N.; Monowar, M.M. Survey of Centralized and Decentralized Access Control Models in Cloud Computing. *Int. J. Adv. Comput. Sci. Appl.* **2021**, *12*, 339–346. [CrossRef]
25. Shan, T.L.; Ismail, S.A.; Azizan, A. Access Control Models for Cloud Computing: A Review. In Proceedings of the 2018 2nd International Conference on Telematics and Future Generation Networks, TAFGEN, Kuching, Malaysia, 24–26 July 2018; pp. 155–158. [CrossRef]
26. Cai, F.; Zhu, N.; He, J.; Mu, P.; Li, W.; Yu, Y. Survey of access control models and technologies for cloud computing. *Clust. Comput.* **2019**, *22*, 6111–6122. [CrossRef]
27. Aftab, M.U.; Hamza, A.; Oluwasanmi, A.; Nie, X.; Sarfraz, M.S.; Shehzad, D.; Qin, Z.; Rafiq, A. Traditional and Hybrid Access Control Models: A Detailed Survey. *Secur. Commun. Netw.* **2022**, *2022*. [CrossRef]
28. Aluvalu, R.K.; Muddana, L. A survey on access control models in cloud computing. *Adv. Intell. Syst. Comput.* **2015**, *337*, 653–664. [CrossRef]
29. Liu, Z.; Gu, W.; Xia, J. Review of access control model. *Comput. Mater. Contin.* **2020**, *61*, 43–50. [CrossRef]
30. Saaty, T.L. The analytic hierarchy and analytic network measurement processes: Applications to decisions under Risk. *Eur. J. Pure Appl. Math.* **2007**, *1*, 122–196. [CrossRef]
31. Saaty, T.L. What is the analytic hierarchy process? In *Mathematical Models for Decision Support*; Springer: Berlin/Heidelberg, Germany, 1988; pp. 109–121.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.