Hindawi
Wireless Communications and Mobile Computing
Volume 2021, Article ID 9957214, 17 pages
https://doi.org/10.1155/2021/9957214

Research Article

T-RBAC Model Based on Two-Dimensional Dynamic Trust Evaluation under Medical Big Data

Rong Jiang,[1,2,3] Yang Xin,[1,2,3] Huiping Cheng,[4] and Wenxuan Wu[1,2,3]

[1]*Yunnan University of Finance and Economics, Kunming, China*
[2]*Key Laboratory of Service Computing and Safety Management of Yunnan Provincial Universities, Kunming, China*
[3]*Kunming Key Laboratory of Information Economy & Information Management, Kunming, China*
[4]*Northwest University, Xi'an, China*

Correspondence should be addressed to Huiping Cheng; chenghuiping@nwu.edu.cn

Received 12 March 2021; Accepted 29 July 2021; Published 15 August 2021

Academic Editor: M. Hassaballah

Copyright © 2021 Rong Jiang et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

The professionalism and complexity of medical big data and the expensiveness of acquiring medical knowledge make it difficult for policymakers to judge whether the information accessed by doctors is necessary from a professional perspective and to formulate accurate access control strategies. To solve the above problems, this paper proposes a T-RBAC (trust-role based access control) model based on two-dimensional dynamic trust assessment, Using AHP and Grey theory to quantify the role attribute trust in the dimension of the doctor's own attributes, Using Euler's measurement method and probability statistics to quantify doctors' behavioral trust in the dimension of historical behavior, then, the trust rule base performs hierarchical authorization based on the comprehensive trust value obtained by the weighted average. Multiattribute trust comprehensive evaluation makes the access control model have finer access granularity and higher security. At the same time, the introduction of time decay function and penalty function enhances the model's sensitivity, dynamics, and resistance to bleaching attacks.

1. Introduction

With the development of the new generation of mobile Internet and the Internet of Things, data processing capabilities continue to increase, computing, and storage costs continue to decrease, and networks continue to expand. In particular, high-tech technologies such as artificial intelligence and sensor equipment have gradually integrated into the medical industry. Medical informatization has entered a period of rapid development and has accumulated massive structured and unstructured medical data. The popularization of HIS (hospital information system) integrates data scattered in various departments of medical institutions or among medical institutions and stores them in a unified manner, realizes data sharing, facilitates information access, and improves the modern management level and diagnosis and treatment of medical institutions. Efficiency played a huge role and became an indispensable technical means in medical activities [1]. Traditional medical data mainly comes from a large amount of data generated in hospitals and other medical institutions when patients seek medical treatment, including various outpatient and emergency records, hospitalization records, imaging records, laboratory records, medication records, surgical records, and medical insurance data [2]. As shown in Figure 1, with the deepening of informatization, medical big data under the background of "Internet + medical" mainly comes from four aspects: patient treatment process (patient-centered data generated during the routine clinical diagnosis and management of the hospital, such as physical sign data, laboratory test data, patient description data, surgical data, and cost data), wearable devices (sports health: Apple Watch, Google Glass, Sports Bracelet; medical health: vision and hearing enhancers, pacemakers, ECG monitors, and other

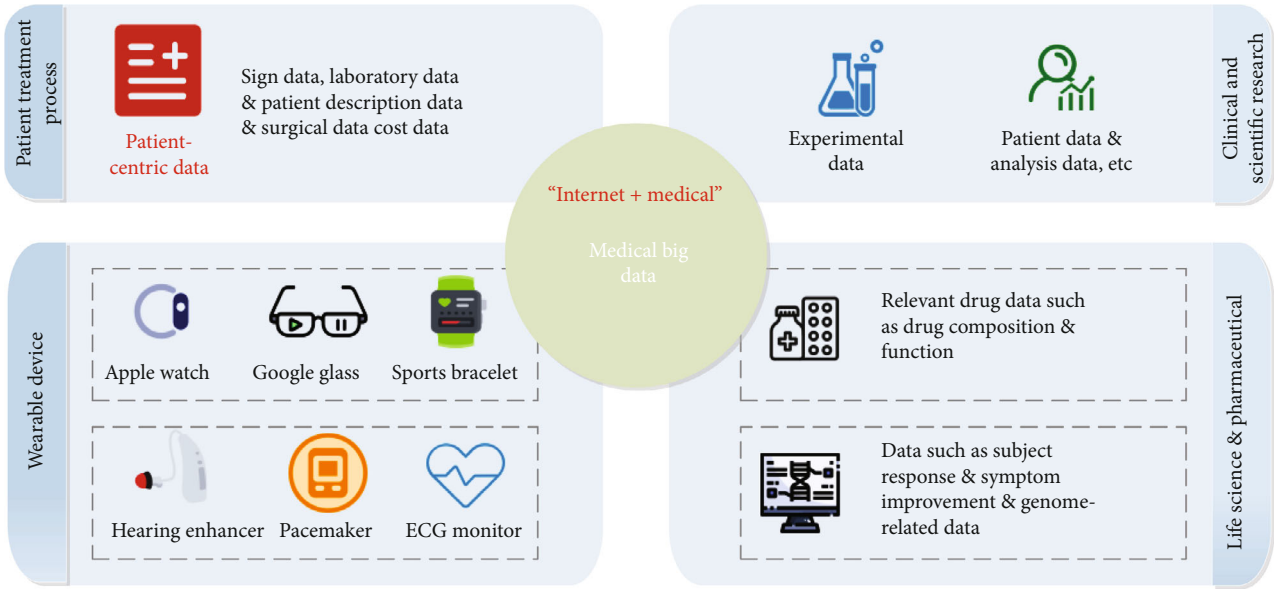

Figure 1: Main sources of medical big data.

medical-grade wearable devices), clinical research and scientific research (produced in experiments data, including data generated by some patients), life sciences and pharmaceuticals (data generated in experiments, drug components and effects, and other related drug data; data on subject response and symptom improvement, and genome-related data, etc.).

Medical big data not only has the data characteristics of traditional big data: large quantity, diversity, rapidity, and value, but also has special attributes of the medical industry: polymorphism, timeliness, incompleteness, sensitivity, and closure [3]. There are various forms of medical data, including pure data such as disease description, laboratory data, and medical expenses, as well as signal atlas data like electrocardiogram atlas, as well as image data such as X-ray and CT, and video data generated by ultrasound diagnosis during pregnancy. They are all constantly changing data in the time dimension and have a strong temporality. In the process of doctor-patient interaction, the doctor's subjective judgment bias and the patient's unclear description of their symptoms will cause incomplete medical data. As a kind of data based on "personal attributes," medical data has higher sensitivity and privacy than ordinary data. Therefore, many hospital clinical data systems are relatively independent local area networks, or even external networks, independent autonomous systems leading to "information islands."

The application and development of medical big data is conducive to saving medical costs and improving the level of medical services, which will have a great impact on the economy, society, and people's lives, especially in clinical auxiliary diagnosis and treatment, health management, precision medicine, and infectious disease monitoring aspect [4]; all countries are vigorously promoting the application of medical big data, but the security risks that follow are becoming more and more serious. In order to investigate how people perceive and balance the benefits and damages to patients from sharing patient electronic health data, Gihan [5] conducted a large number of questionnaires on doctors and patients: Most people (90%) agree to share patient health records and provide clinical advice; but more than 70% of these people do not want these data to be shared outside the hospital, and more importantly, only a few people (38%) believes that electronic records are more private than paper records, which reflects people's concerns and doubts about the security of their private information. As medical data is more sensitive and private than ordinary data, it is hard to imagine the harm and loss caused by information leakage. For example, the data of the health agency in Utah in the United States was stolen, causing the information leakage of more than 180,000 people [6], resulting in extremely bad social impact and a crisis of trust. In addition to the data leakage caused by external intrusion and stealing of medical information through security vulnerabilities in the medical information system, there is also a more common and more harmful data leakage situation: information abuse or permission abuse within the system, which results in patient privacy damaged leaks. Compared with paper medical records, patient information in the health information system, such as electronic medical records, can be quickly modified, deleted, copied, and pasted, and it is not easy to find [7].

Information silos and data leakage are problems that must be faced in the development of big data in the medical field. The root cause is the lack of mature privacy protection theories and mechanisms that match them. Therefore, how to use various technologies to ensure the security and privacy of medical data is the focus and difficulty of medical big data research. Currently, the commonly used technologies in terms of data privacy and security protection include [8] identity authentication, data encryption, data desensitization, and access control technologies. The 2017 Verizon Data Breach Investigations Report (DBIR) showed that the medical industry has ranked first in information leakage, and it is also the only industry in which internal threats are higher

than external threats. The threats mainly come from excessive access caused by improper allocation of access rights for medical staff. Therefore, compared with other technologies, access control technology can better solve the root problem: data leakage and abuse caused by improper allocation of access permissions. This is undoubtedly one of the most effective methods for protecting the privacy of medical and health big data. As the main producer and user of medical data, how to formulate scientific access control strategies to prevent the leakage of patient privacy is particularly critical for hospitals. Traditional access control mostly involves security administrators formulating access rights allocation strategies based on experience. This kind of access control authorization behavior itself is a labor-intensive task that requires a lot of energy from policymakers. Medical data in the context of big data has the characteristics of strong professionalism, large amount of information, multiple types of information, and fast update speed. The formulation of access strategies has been difficult to achieve through traditional methods.

In order to solve the above problems, some scholars have proposed a trust-based access control method [9–11]; Singh et al. propose a trust access control model for EHS. They have added user trust into the identity-based access control (IBAC) model. For the computation of user trust, they used a beta reputation approach. However, this solution cannot resist concealed attacks such as bleaching attacks. Due to the sensitivity and openness of EHS, these solutions are not sufficient to provide complete security.

The contribution and innovation of this article is to address the above medical data privacy leakage problem, combined with appropriate mathematical theory and methods to provide a targeted and effective access control model; the specific model is as follows:

(1) Uses analytic hierarchy process (AHP) to layer the doctor's own trust indicators and calculate the weights, and the definite weighted functions is used to comprehensively evaluate the trust indicators to obtain the doctor's role attribute trust

(2) Use probability theory and Euler distance measurement method to quantify the trust of medical records in the medical system to obtain the trust value of the doctor's historical behavior and comprehensively quantify the trust value with the role attribute trust to obtain the comprehensive trust value

(3) Introduction of the penalty factor and the time decay function enhances the trust algorithm's ability to resist bleaching attacks and ensures the objective law of slow increases and sharp drops in reputation values. Combine the two-dimensional trust evaluation algorithm with the T-RBAC model and finally get a fine-grained access control model that is more suitable for the medical big data background

The rest of this article is organized as follows. Section 2 describes the current research status of trust evaluation and access control and analyzes the progress and deficiencies of related research in the context of medical big data. Section 3 introduces the data leakage problems and security risks in the doctor's work process and the corresponding strategies given in this paper. Section 4 introduces the construction of the index system of doctor trust and the specific methods of various trust quantification. Section 5 conducts related experiments on the algorithm model from three aspects of effectiveness, sensitivity and safety and conducts a comparative analysis of performance. Section 6 summarizes this article.

2. Related Work

Most scholars at home and abroad have conducted research on access control based on big data. For example, in order to solve the problem of frequent access and inefficiency of subject and object in the big data environment, scholars such as Huang [12] classify the roles of the server and assign different roles according to the different access objects and then perform different permissions in the task allocation stage. The classification improves efficiency to a certain extent. On this basis, Zhang et al. [13] proposed an access control model that evaluates risks and benefits. This model no longer only performs access control based on fixed permissions assigned in advance but starts to measure whether the risk generated by access behavior is less than the benefits brought by, and whether the risk is tolerable by the system, if some unknown access behavior occurs, and the risks and benefits generated by the behavior are evaluated; the system can still be accessed. It is very necessary for applications and can greatly improve its usability. In order to meet the security and privacy requirements of the multitenant Hadoop ecosystem, Gupta et al. [14] proposed a HeABAC model that can be applied to multiple trust scenarios. Gupta et al. [15] adds object tags as object attributes to the RBAC model in the Hadoop ecosystem and proposes a role access control (OT-RBAC) model based on object tags. This model only adds object attributes and does not consider the impact of subject attributes and environment attributes on access authorization. Moreover, this access control model still cannot solve the problem of automatic and targeted adjustments in the medical information system according to the doctor's behavior. [16] proposes and evaluates a hybrid monitoring solution (SecHMS). The hybrid monitoring solution (SecHMS) uses public key encryption and hashing techniques to provide data security in cloud computing. This solution allows users to continuously monitor the stored data, so they trust the cloud computing system more. But if placed in a special environment such as medical information, this solution means that patients need to continue to authorize their data and decide to provide it to doctors to reduce the risk of medical information leakage. This is obviously very cumbersome and troublesome, and this is not conducive to the development of medicine to some extent. [17] proposes the federated access control reference model (FACRM) to formalize the design of secure BD solutions within the Apache Hadoop stack. The research of this paper has indeed brought great help to the problems within the scope of security and privacy of the Hadoop stack. However, the current role of Hadoop

commonly used in the medical field is to assist diagnosis and personalized treatment. The medical information system based on Hadoop is not widely used, so Hadoop access control should be considered in the future in the medical field. Compared with ordinary big data, medical big data has higher sensitivity and value density and requires a more precise and fine-grained authorization mechanism. Therefore, many access control methods and theories applicable to the background of big data cannot be applied well to medical big data. Although there are few related researches applied to the medical field, some scholars have done research on it. Wilikens et al. [18] proposed a context-sensitive authorization and access control method based on RBAC to simplify the complex authorization problem of large amounts of data, but the data type of medical big data is too complex and too professional, and a single RBAC access control technology has its authority classification. There are great difficulties in setting, setting and grading information, and eventually the mining and assignment of roles will become an extremely difficult task. Based on this, literature [6, 19] introduces risk into the access control scheme, divides doctors into honest and malicious doctors, uses information entropy to describe doctors' behavior, and assigns the entropy of doctors' visit behavior as a tolerable risk quota to each doctor. This solution is a relatively loose access control method, which greatly reduces the workload of the administrator, but the effect of access control with too coarse granularity is not ideal. Compared with risk, trust can more closely describe the relationship between the producer, manager, and user of medical data. Trust refers to the subjective willingness of the requesting party to accept the disadvantaged position of the trusted party in the absence of the ability to supervise and control the other party's behavior and expect the trusted party to take actions that are beneficial to itself [20]. The construction of the relationship of trust always involves the weaker and stronger parties. If there is no weaker party, there is no need for trust. Obviously, the cost of acquiring medical knowledge is very expensive; patients and interview strategy makers are in a weak position because they do not have enough theoretical knowledge to judge whether the information accessed by doctors is really necessary. In short, the relationship between patients, interview strategy makers, and doctors is that the former two actively accept the disadvantaged position but expect not to be harmed. At the same time, compared with sensitive data, whether to trust the visitor is more optimistic and more in line with the theoretical logic than whether the visitor can bear the risks brought by the visit. Therefore, in order to achieve more secure, flexible, and fine-grained access control, scholars at home and abroad began to try to integrate the "trust" mechanism into the traditional access control model and formulated corresponding security strategies according to different trust levels [21] .In 2006, Chakraborty and Ray [22] introduced a trust evaluation model on the basis of static RBAC and proposed a trust-role-based access control scheme (trust-role-based access control (Trusr-RBAC)), but its user trust level. It is preset and will be reevaluated only when the role changes. Therefore, the dynamics of trust measurement is not strong, and the granularity of access control is relatively coarse. On this basis, Hongyu et al. [23] proposed a Trust-RBAC model with finer granularity, which provides authorization trust constraints, integrates entity trust and behavior trust, and designs a comprehensive multifactor user credibility evaluation program. Banyal et al. [24] proposed an access control model based on user trust in the cloud environment, which divided user trust into static trust and dynamic trust. However, this model is vulnerable to attacks from external clouds, and its access strategy and authorization management design are weak. Yang and Yu [25] analyzed the characteristics of the user's visit behavior and the factors that affect the user's credibility and gave an evaluation index of the user's behavior credibility. Yuanbing et al. [26] layered the attributes related to trust in the cloud environment and introduced the trust evaluation of a third-party expert group to integrate subjective trust and objective trust into the trust evaluation process. Trust is regarded as the basic relationship between doctors and patients in academia, so it has always been a research hotspot in the medical field at home and abroad. Among them, the research team headed by Hall and M. A of Wake Forest University and the Trust Study Group research team represented by Thom and D.H. of Stanford University have conducted a lot of trust-related research as early as the 1990s [20]. Peadboy clarified the important position and significance of trust in the medical field in his discussion. Vawdrey [27] introduces trust into the healthcare information system, establishes an identity verification and access control service framework based on trust negotiation, and explains the importance of trust evaluation when performing sensitive matters and the huge potential of trust evaluation in ensuring the security of future medical systems. With the widespread application of telemedicine technology, wireless and mobile networks, Boukerche and Ren [28] proposed a trust evaluation model for mobile electronic medical systems, which conducts trust evaluation on the behavior of each node, thereby preventing node misbehavior. References [9, 29, 30] have all made relevant studies on the medical trust evaluation model and achieved certain results, but the problems of weak dynamics and sensitivity of access control model still need to be further studied. The effect of trust-based access control applied to medical big data is relatively prominent, so it has attracted the attention of a large number of scholars, and some scholars have conducted in-depth research on it, but these solutions still have the following shortcomings in the application of the medical field [21]: ① A single trust evaluation algorithm cannot simultaneously reflect the dynamics and sensitivity of trust. ② The existing user behavior trust evaluation algorithm does not reflect the objective law of slow increase and sudden decrease of trust value and its ability to resist bleaching attacks is weak. ③ The existing trust evaluation algorithms are mainly combined with the static RBAC model and lack of research on the combination with the dynamic T-RBAC model. In response to the above problems, this paper uses the gray system theory, probability theory, and Euclidean distance to comprehensively quantify the doctor's trust value and introduces a penalty factor and attenuation function to build a more flexible, safer, and more bleach-resistant fine-grained

trust evaluation algorithm, so the research in this article is an important supplement to the research of medical big data access control.

3. Related Question

This part mainly analyzes the problems existing in the establishment of the medical big data access control model and the deficiencies of the algorithms proposed by other scholars and propose the solutions for the behavior of doctors' disclosure of patients' privacy during medical visits. Doctors are the main users of the medical system. We divide it into three parts: "honest doctor," " malicious doctor," and "changing doctor." When honest doctors work, they only select work targets related to the patient's condition and access patient information related to work targets. On this basis, "malicious doctors" and "changing doctor" will try to illegally obtain more information from patients. When formulating access control policies, we need to understand what behaviors may cause information leakage. According to the characteristics of these behaviors, corresponding environmental constraints are added during access control to reduce the risks caused by this behavior. The specific content is as in Question 1. At the same time, it is also necessary to study the reasons for the bias of model trust evaluation in the trust model and perform corresponding optimizations to improve the evaluation performance of the model, as described in Question 2 and Question 3.

Use the following symbols to formally describe related issues in this section:

γ: the types of doctors, and $\gamma = \{h, m, c\}$; the main types involved in this article are honest doctor h, malicious doctor m, and changing doctor c

D: set of doctors

R: set of doctor's medical records in HIS

M: set of patient information;

TP: set of time periods

D_γ: set of different types of doctors, and $D_\gamma \subset D$

$T_{\text{total}}(r)$: the number of mission targets established in the medical record r

$\varphi(T_i, M_i)$: the degree of correlation between the target T_i and the access information M_i

$B_{\text{H-risk}}$: high-risk visits by doctors

Question 1. Malicious doctors may try to forge more job objectives, or try to obtain more patient information under the same job objective. Falsified job objectives and the behavior of reviewing unnecessary patient information will lead to the disclosure of patient privacy. The purpose of this article is to avoid doctors' access to unnecessary medical data.

Ideally, doctor d should follow the "principle of least privilege" during the diagnosis and treatment of patients, and the access authority P should be limited to the access authority of relevant information under the current task target T, and $P = P^d_{\min}(T)$. However, in actual work, it is difficult to achieve precise division and grant of permissions under the background of medical big data. In order to prevent the doctors from being assigned too few access permissions and obstructing the doctor's work, $P > P^d_{\min}(T)$ and $P \ggg P^d_{\min}(T)$ are common in the assignment of permissions. This will result in the high-risk behavior $B_{\text{H-risk}}(T)$ in which the malicious doctors forge more work targets in order to obtain more privacy information of patients or the high-risk access behavior $B_{\text{H-risk}}(\varphi)$ in which the malicious doctors try to access more information under the same work target [6].

Formally, $T_i \in T$, $r \in R$, $T_{\text{total}}(r) = \sum_{i=1}^{n} T_i \geq 1$, $B_{\text{H-risk}}(T) \propto T_{\text{total}}(r)$, and $T_{\text{total}}(r) \longrightarrow B_{\text{H-risk}}(T)$; $\forall T_i \in T$, $M_i \subset M$, $B_{\text{H-risk}}(\varphi) \propto \varphi(T_i, M_i)$, $\varphi(T_i, M_i) \longrightarrow B_{\text{H-risk}}(\varphi)$, Finally, the doctor's high-risk visit behavior $B_{\text{H-risk}}$ is formalized as $B_{\text{H-risk}} = B_{\text{H-risk}}(T) + B_{\text{H-risk}}(\varphi)$.

The first thing to be clear is that when $T_{\text{total}}(r) > 1$ does not mean that it must be a high-risk behavior. In the actual diagnosis, T is established based on the doctor's judgment on the patient's condition and combined with his own experience, which has great uncertainty. Misdiagnosis may occur, so sometimes it is necessary to continue to establish and overthrow the preset goals until the final treatment task is completed. However, compared with the honest doctor D_h, the malicious doctor D_m prefers to forge more preset targets to obtain more information, that is, $T^{D_m}_{\text{total}} \ggg T^{D_h}_{\text{total}}$. Therefore, it is reasonable to take the relevance of the target information and the achievement rate of the information target as the trust index of the visit behavior in this paper.

Question 2. In the medical information system, such a situation may arise: doctors who have had bad behaviors in the past no longer have the risk of privacy leakage, or the honest doctors in the past now have the risk of privacy leakage. Therefore, how to evaluate the impact of doctors' historical behavior on the present and future is also a question that needs to be discussed in our paper.

Let $\text{TP} = \text{TP}(\text{last}) + \text{TP}(\text{now}) + \text{TP}(\text{future})$, $\forall tp_i \in \text{TP}(\text{last})$, $\forall tp_j \in \text{TP}(\text{now})$, $\forall tp_k \in \text{TP}(\text{future})$. In an ideal state, the interview behavior of honest doctor D_h should satisfy $B_{\text{H-risk}}(tp_i) + B_{\text{H-risk}}(tp_j) + B_{\text{H-risk}}(tp_k) = 0$. The visit behavior of the malicious doctor D_m is defined as $B_{\text{H-risk}}(tp_i) \gg 0$, $B_{\text{H-risk}}(tp_j) \gg 0$, $B_{\text{H-risk}}(tp_k) \gg 0$. But in reality, there is a third type of doctor we call "changing doctor" D_c. D_c, as a doctor type independent of D_m and D_h, is more like a product of the conversion between D_m and D_h. It refers to the doctor who used to be a malicious doctor, and the recent visit behavior has become normal, and there is a tendency to transform to an honest doctor, or a doctor who was an honest doctor in the past, and recently started to visit abnormally and tends to be a malicious doctor. Therefore, even if a doctor has decided to become an honest doctor, his poor access behavior in the past has affected his trust assessment, and his access rights are still restricted. So, how to measure the degree of influence of medical records in different time periods on their trust evaluation to make the trust evaluation mechanism more sensitive is a problem faced by medical records as the basis for trust evaluation.

To solve this problem, this paper uses the attenuation function to assign its weight. The shorter the visit record time, the greater the weight and the higher the influence on the doctor's trust evaluation. The longer the visit record time,

the smaller the weight, the lower the influence on the doctor's trust evaluation. Using this method can improve the timeliness and dynamics of the evaluation model and reduce the impact of unstable doctors' past legal or illegal behaviors on their current trust evaluation. It also conforms to the objective fact that the longer the medical record, the lower the reference value. The specific implementation methods and steps will be introduced in Section 4.

Question 3. Quantify doctors' behaviors from multiple perspectives as the basis for trust evaluation.

Most of the trust assessments of role abilities are automatically quantified according to certain standards. The benefits are obvious; especially in the big data environment, this automated method can be faster and simpler, greatly reducing the workload of managers. However, the effect of this method on the role attribute trust evaluation of medical staff is very poor. The main reason for this phenomenon is the unequal evaluation scale caused by the complexity of division of departments. For example, working years can be used as a major factor to measure the core competitiveness of medical staff. Compared with nurses and surgeons, the contribution of the same one year of work experience to their core competitiveness is not equivalent, so the same evaluation indicators in different professional fields The scale level is different; therefore, this paper uses a combination of expert evaluation and gray theory to avoid this problem when evaluating the trust of role attributes. Compared with the visit behavior, the doctor's role attributes have less fluctuations in a certain period, so there is no need to perform frequent role attribute trust evaluation and replacement. It only needs to be updated regularly. The replacement cycle is set according to the needs, such as monthly, quarterly, and yearly.

Therefore, the human evaluation of the doctor's role attribute trust will not greatly affect the automation of the model. On the contrary, the expert scoring can further improve the scientificity and accuracy of the model.

4. Two-Dimensional Dynamic Trust Quantification

4.1. Algorithm Idea. This paper proposes a two-dimensional dynamic trust (RT, HT) evaluation algorithm based on T-RBAC. The T-RBAC model is combined with the characteristics of the medical big data environment and the doctor's workflow, and the influence of factors such as the doctor's own trust attributes and historical behavior credibility on trust is comprehensively considered. The algorithm measures the credibility of doctors in two dimensions: (1) using AHP and gray theory to layer the doctor's own trust attributes and quantify the role attribute trust RT and (2) the Euler distance measurement method is used to measure the similarity of medical records, and the time attenuation function is introduced to calculate the time attenuation weight w_t and the medical record trust degree ReT. Analyze the doctor's historical visit behavior performance through probability statistics, and add the trust Penalty policy, and finally get the historical behavior trust HT. According to the weights ω_{RT} and ω_{HT} set in advance by the system, RT and HT are weighted and averaged to obtain the doctor's comprehensive trust degree CT, $CT_{dr} = \omega_{RT} \bullet RT_{dr} + \omega_{HT} \bullet HT_{dr}$. Moreover, ω_{RT} and ω_{HT} can be adjusted according to demand, but in order to ensure that both RT and ReT can exert their due effects, their parameter settings should meet the following constraints: $\omega_{RT}, \omega_{HT} \in [0.4,0.6]$, $\boxplus \omega_{RT} + \omega_{HT} = 1$. Finally, trust rule base (TRB) assigns corresponding access rights according to preset access rules, as shown in Figure 2.

TRB presets four trust intervals $[T_1, T_2)$, $[T_2, T_3)$, $[T_3, T_4)$, and $[T_4, T_5]$ according to the system to correspond to different levels of authorization rules R_1, R_2, R_3, and R_4. According to the trust interval to which the comprehensive trust degree CT belongs, the authorization rule R_x of the corresponding level is activated, so as to achieve the purpose of access control. The value of the interval threshold T_x can be flexibly set according to actual needs. The T_x of TRB in this article are $T_1 = 0$, $T_2 = 0.6$, $T_3 = 0.8$, $T_4 = 0.9$, and $T_5 = 1.0$. Specific authorization rules are shown in Table 1.

This paper adopts a two-dimensional trust (RT, HT) evaluation strategy, which has a finer granularity than the previous one-dimensional trust evaluation strategy. The introduction of time decay weight w_t and punishment strategy can improve access control to roles, tasks, access behaviors, etc. The dynamic adaptability and sensitivity of factors and the ability to resist bleaching attacks were included.

4.2. Role Attribute Trust

4.2.1. Construction of Role Trust Indicators

Definition 1. Doctor attribute trust value RT. RT refers to the trust-related attributes inherent in doctors themselves.

From a psychological point of view, trust refers to a person's grasp of the credibility of another person. When assessing the trust of doctors by patients and access control strategy makers, in addition to direct trust in doctors' historical behaviors, they also consider indirect trust in doctors' abilities such as skills, talent, sense of responsibility, and attitude, and finally decide whether to trust doctors. In general, the weaker party is more willing to trust a doctor with strong ability when other conditions are unknown or the same. Therefore, it is necessary and consistent with objective laws to quantify the role attributes of doctors.

This article consulted hospital experts and university experts in related fields, and based on the literature [20, 21], combined with the characteristics of doctors in the context of big data, according to the affiliation between each attribute, from the core competitiveness and interpersonal quality analyze the attributes of doctors layer by layer, and establish a trust attribute tree based on the doctor's trust attributes. As shown in Figure 3, $T = \{T_1, T_2\}$ is the first-level trust attribute, and $T_1 = \{t_{11}, t_{12}, t_{13}, t_{14}\}$ and $T_2 = \{t_{21}, t_{22}, t_{23}\}$ are the second-level trust attribute.

4.2.2. Determination of the Weight of Trust Attribute Index. When evaluating the trust attributes of doctors, because the importance of each index is different, the role of evaluating doctors' trust value is also different. The role attribute trust evaluation of doctors is a goal evaluation under the influence

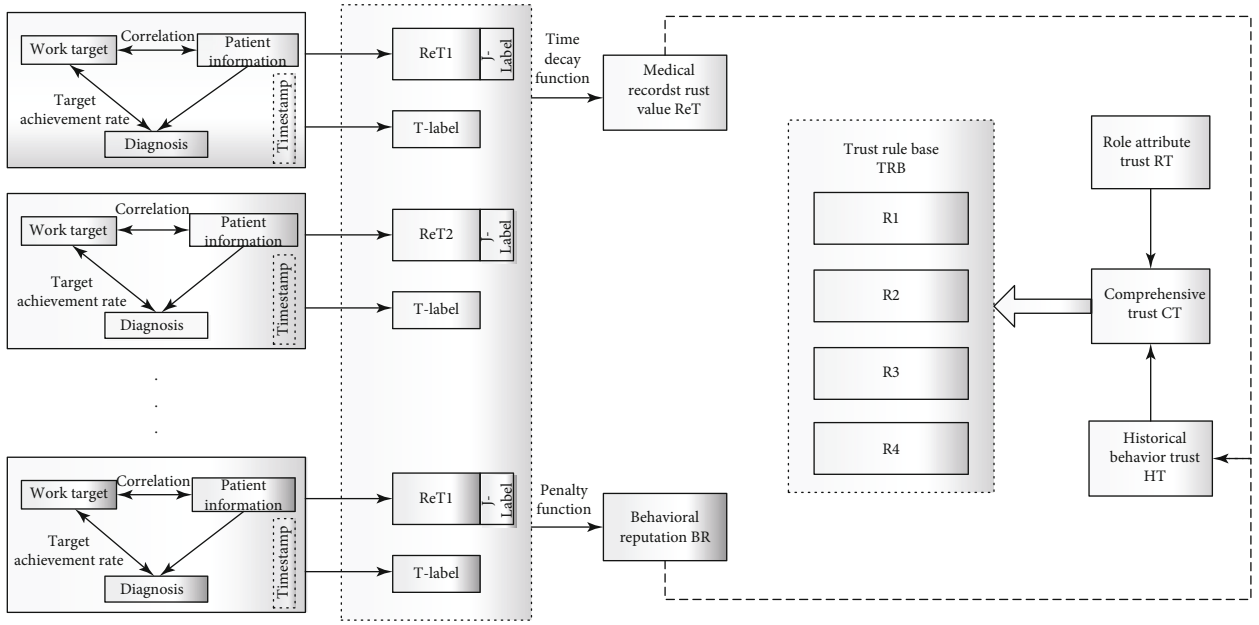

Figure 2: Two-dimensional dynamic trust quantification algorithm.

Table 1: Rule base permission distribution table.

Authorization level	Linguistic definition	Confidence interval	Permission assignment
R_1	Very credible	$0.9 \le x \le 1.0$	Allow 10% excess access
R_2	Credible	$0.8 \le x < 0.9$	Allow 5% excess access
R_3	Untrustworthy	$0.6 \le x < 0.8$	Excessive access is not allowed
R_4	Very untrustworthy	$0 \le x < 0.6$	Deny user's access request

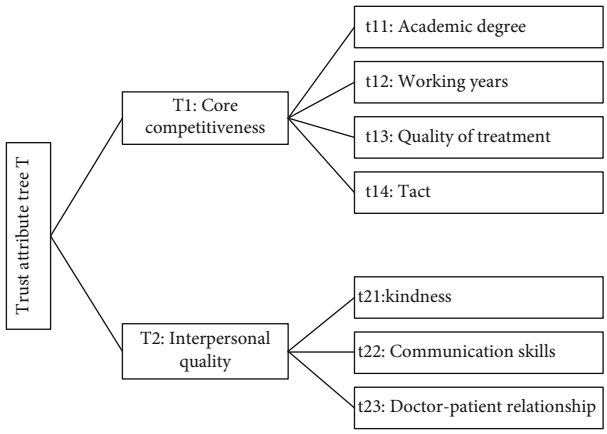

Figure 3: Attribute tree of doctor role attribute trust.

of multiple factors, which is a "Multiobjective decision-making problem," so this article uses AHP to determine the weight [31]. Specific steps are as follows.

Step 1. Establish a role attribute trust judgment matrix. According to the affiliation of each attribute in the trust attribute tree, all the doctor's trust attributes are divided into three levels. The highest level s_1 contains one element, the root node T; the middle level s_2 contains two elements $\{T_1, T_2,\}$, and the lowest level s_3 contains Several elements $\{t_{11}, t_{12}, t_{13}, t_{14}, t_{21}, t_{22}, t_{23}\}$. Using the method of pairwise comparison, scoring is based on the relative importance of elements at this level and establish the doctor's kth level trust attribute judgment matrix A_{sk} and $1<k \le 3$ is expressed as

$$A_{sk} = \begin{bmatrix} a_{11}^k & a_{12}^k & \cdots & a_{1j}^k \\ a_{21}^k & a_{22}^k & & a_{2j}^k \\ \vdots & & \ddots & \vdots \\ a_{i1}^m & & \cdots & a_{ij}^k \end{bmatrix}. \quad (1)$$

At the same time, the idea of comparing index weights in pairs can greatly reduce the impact of human judgment errors on the evaluation process [32, 33]. When constructing the judgment matrix A_{sk}, the importance of different trust attributes is represented by a sequence of 1-9 natural numbers. The specific scaling methods and meanings are shown in Table 2.

Table 2: Scale and meaning of judgment matrix of analytic hierarchy process.

Scaling	Meaning
1	Compared with the two trust attributes, they are of equal importance
3	Compared with the two trust attributes, one attribute is slightly more important than the other
5	Compared with the two trust attributes, one attribute is obviously more important than the other
7	Compared with the two trust attributes, one attribute is more important than the other
9	Compared with the two trust attributes, one attribute is extremely important than the other
2, 4, 6, 8	The scale when taking a compromise between two adjacent scales
Reciprocal	If the attribute i is compared with the attribute j, the importance scale value is a_{ij}, the importance of attribute j relative to i is $a_{ji} = 1/a_{ij}$

Step 2. According to the judgment matrix, calculate the relative weight. The judgment matrix constructed by the 1-9 scale method is used to calculate the weight of each index by the root finding method.

(1) Calculate the product of row elements of the judgment matrix

$$M_i^k = \prod_{j=1}^{n} a_{ij}^k, \quad i = 1, 2, \cdots, n \tag{2}$$

(2) Take the continuous product vector M_i^k to the power of n

$$\begin{aligned} M_i^k &= \left(m_1^k, m_2^k, \cdots, m_n^k\right)^T, \\ m_i^k &= \sqrt[n]{M_i^k} \end{aligned} \tag{3}$$

(3) Normalized processing to get the weight vector W^k

$$\begin{aligned} W^k &= \left(w_1^k, w_2^k, \cdots, w_n^k\right)^T, \\ w_i^k &= \frac{m_i^k}{\sum_{i=1}^{n} m_i^k}, i = 1, 2, \cdots, n, \end{aligned} \tag{4}$$

where w_i^k is the weight coefficient of each index of the kth layer, and W^k is the weight vector

Step 3. Consistency check. In order to test the coordination between the importance of each index, it is necessary to check the consistency of the weight coefficient w_i of each layer, and calculate the consistency index CI in (5) and the consistency ratio CR in (6).

$$\mathrm{CI} = \frac{(\lambda_{\max} - n)}{(n-1)}, \tag{5}$$

$$\mathrm{CR} = \frac{\mathrm{CI}}{\mathrm{RI}}, \tag{6}$$

where $\lambda_{\max}$ is the maximum eigenvalue of the judgment matrix A, RI is the average random consistency index, and the value of RI is shown in Table 3.

When calculating the consistency ratio CR, the smaller the CR, the better the consistency of the judgment matrix. When CR < 0.1, it is deemed to have satisfactory consistency. Otherwise, the judgment matrix needs to be revised until the test conditions are met before proceeding to the next step.

4.2.3. Trust Quantification of Role Attributes. The evaluation sample matrix is established according to the expert's score, and the Grey White function is used to quantify each index, and the doctor role attribute trust value RT is obtained. Specific steps are as follows.

Step 1. Calculate the sample matrix through expert scoring method. The evaluation of the trust value of each indicator is completed by experts in the field. The experts score the trust indicators according to their own experience and relevant domain knowledge, and fill in the scoring table. The final sample matrix d as

$$d = \begin{bmatrix} d_{11} & d_{11} & \cdots & d_{1n} \\ d_{11} & d_{11} & & d_{1n} \\ & \vdots & \ddots & \vdots \\ d_{m1} & d_{m2} & \cdots & d_{mn} \end{bmatrix}. \tag{7}$$

Step 2. Determine the evaluation gray category. Determining the evaluation gray class is to determine the number of evaluation gray classes, the gray class gray number and the White function $f(x)$, which are divided into 5 gray classes according to the degree of trust $s = \{1, 2, 3, 4, 5\}$ and use the equal difference scoring method.

Table 3: Average random consistency index RI table.

Order	1	2	3	4	5	6	7
RI	0	0	0.52	0.89	1.12	1.26	1.36
Order	8	9	10	11	12	13	14
RI	1.41	1.46	1.49	1.52	1.54	1.56	1.58

The first gray category: $s = 1$

$$f_1(x) = \begin{cases} x, & x \in [0, 1], \\ 2 - x, & x \in [1, 2], \\ 0, & x \notin [0, 2]. \end{cases} \tag{8}$$

The second gray category: $s = 2$

$$f_2(x) = \begin{cases} \dfrac{x}{2}, & x \in [0, 2], \\ \dfrac{4 - x}{2}, & x \in [2, 4], \\ 0, & x \notin [0, 4]. \end{cases} \tag{9}$$

The third grey category: $s = 3$

$$f_3(x) = \begin{cases} \dfrac{x}{3}, & x \in [0, 3], \\ \dfrac{6 - x}{3}, & x \in [3, 6], \\ 0, & x \notin [0, 6]. \end{cases} \tag{10}$$

The fourth gray category: $s = 4$

$$f_4(x) = \begin{cases} \dfrac{x}{4}, & x \in [0, 4], \\ \dfrac{8 - x}{4}, & x \in [4, 8], \\ 0, & x \notin [0, 8]. \end{cases} \tag{11}$$

The fifth gray category: $s = 5$

$$f_5(x) = \begin{cases} \dfrac{x}{5}, & x \in [0, 5], \\ 1, & x \in [5, +\infty]. \end{cases} \tag{12}$$

Step 3. Calculate the gray evaluation coefficient to construct the gray evaluation weight matrix. The trust evaluation index t_{ij} of doctor dr, the gray evaluation coefficient belonging to the e-th evaluation gray category is $X_{ije} = \sum_{k=1}^{p} f_e(d_{ij})$, which belongs to the total gray evaluation coefficient of each evaluation gray category is $X_{ij} = \sum_{e=1}^{5} X_{ije}$.

For the evaluation index t_{ij}, the gray evaluation weight value of the evaluation object belonging to the eth gray class is denoted as r_{ije}, then $r_{ije} = X_{ije}/X_{ij}$, which can determine the trust evaluation index t_{ij} for e gray class gray evaluation weight vectors r_{ij}, $r_{ij} = (r_{ij1}, r_{ij2}, \cdots, r_{ije},)$. Then, determine the trust evaluation index T (a set of indexes t_{ij}) for the full matrix R_i of each evaluation gray category gray evaluation.

Step 4. Calculation of the doctor attribute trust value TA. According to the foregoing calculation, the second-level trust index weight W_i is obtained, then the second-level index is comprehensively evaluated $B_i = W_i \times R_i$, and the first-level index gray evaluation matrix $R = (B_1, B_2, \cdots, B_i,)^T$, repeat the above steps to make a first-level comprehensive evaluation $B = W \times R$, and finally get the doctor's role attribute trust value RT after normalization.

4.3. Historical Behavior Trust. The doctor's historical behavior trust value HT includes two aspects: medical record trust ReT and behavior reputation BR. ReT is related to the goal correlation P and the goal achievement rate C. According to P_i and C_i, the trust degree of the ith medical record can be obtained ReT_i, the corresponding weight w_i is assigned through the time-based attenuation function, and the weighted average is used to calculate the doctor. The average historical medical record trust value ReT and use the penalty function to calculate the doctor's behavior reputation BR. Finally, the weighted average of ReT and BR will get the doctor's behavioral trust value HT.

4.3.1. Modeling of Medical Records. Medical records are essentially a mapping of the doctor's work process. The basic process of the doctor's work is as follows: After a simple communication between the doctor and the patient, an expected goal T is determined for the patient based on experience. For example: the doctor dr suspects that patient a is suffering from a certain disease such as "allergic bubble pneumonia" and establishes the corresponding expected target $T_1(a)$; then, the doctor will visit the patient information $M_1(a)$ related to $T_1(a)$ and judge the correctness of $T_1(a)$, if it is correct, the task will be completed; otherwise, set the task target $T_2(a)$ again, and query the patient-related information $M_2(a)$ until the target $T_i(a)$ is confirmed or the patient leaves on their own, every visit. The details are recorded, and a complete medical record is finally formed. And one medical record represents one visit, including several visit (detail) actions. Therefore, according to the doctor's workflow characteristics, the visit records stored in the HIS are modeled as a four-tuple $N = (PN, T, M, Tl)$. The specific meaning of each symbol is as follows.

PN: a set of all patient names

$T(a)$: the set of task goals established by the doctor during the diagnosis and treatment of patient a

$T_i(a)$: the ith expected goal established by the doctor for patient a, and $T(a) = \{T_1(a), T_2(a), \cdots, T_i(a), \cdots, T_n(a)\}$ $(1 \le n \le s)$, and s is the upper limit of the maximum number of mission targets

$M(a)$: the set of all information visited by the doctor during the diagnosis and treatment of patient a

$M_i(a)$: in order to determine the correctness of $T_i(a)$, the doctor accesses the set of patient information, and $M(a) = \{M_1(a), M_2(a), \cdots, M_i(a), \cdots, M_n(a)\}$

$m_i(a)$: the doctor visits the specific information items of patient a, and $M_i(a) = \{m_1(a), m_2(a), \cdots, m_n(a)\}$

$C(a)$: the target completion rate of the medical records generated by the interaction between the doctor and the patient a

Tl: medical record time label

4.3.2. Trust Quantification of Medical Records. When quantifying the trust of doctors' historical medical records, divide their visit behavior into two parts: behavior (actual behavior) and expectation (expected behavior), and quantify trust based on their deviation.

Definition 2. Behavior matrix M. M is a matrix formed by quantifying patient information actually visited by doctors in medical records according to specific standards. M_{T_i} is a first-order matrix composed of the patient information m_i visited by the doctor under the task target T_i quantified according to a specific standard, formally described as (13), the behavior matrix M is composed of i matrices M_{T_i} is formed, as in (14) formula.

$$M_{T_i} = [\rho_1 m_1, \rho_2 m_2, \cdots, \rho_n m_n], \tag{13}$$

$$M = \begin{bmatrix} M_{T_1} \\ M_{T_2} \\ \vdots \\ M_{T_i} \end{bmatrix} (1 \le i \le s). \tag{14}$$

We use the 0-1 variable to mark whether the patient information r has been visited. If it is visited, mark it as $m_i = 1$; otherwise, $m_i = 0$. According to the degree of sensitivity of patient information, it is divided into low-sensitive information, medium-sensitive information, and high-sensitive information and $\rho_{\text{low}} : \rho_{\text{mid}} : \rho_{\text{high}} = 1 : 2 : 3$. The behavior matrix $\rho_{\text{low}} : \rho_{\text{mid}} : \rho_{\text{high}} = 1 : 2 : 3$ is composed of patient information visited by the doctor, so the value of m is all 1. If the number of elements in each row is different, the maximum number of elements is taken as the standard, and the rest is filled with 0.

Definition 3. Expect matrix EM. EM is the information matrix that patients expect doctors to access to complete treatment tasks under the "principle of least privilege." Its information items are consistent with M as follows:

$$EM_{T_i} = [\rho_1 em_1, \rho_2 em_2, \cdots, \rho_n em_n],$$
$$M = \begin{bmatrix} EM_{T_1} \\ EM_{T_2} \\ \vdots \\ EM_{T_i} \end{bmatrix} (1 \le i \le s). \tag{15}$$

In the context of big data, it is impossible to formulate a set of fine-grained expectation matrix judgment criteria based on the Treatment Task-Patient Information, so this paper proposes a judgment method based on probability theory. The idea of this method is on the premise that most doctors are honest, when a large number of doctors visit m under the target T; then, m is the necessary information $m = 1$; otherwise, $m = 0$. Assuming that the proportion of honest doctors in the sample doctor set D is not less than 70%, φ_m^T is the probability that the patient information m is accessed under the target task $T, em = 1(\varphi_m^T > 70\%)$; otherwise, $em = 0(\varphi_m^T \le 70\%)$.

Definition 4. Work goal relevance P. P refers to the degree of relevance between the target T proposed by the doctor and the visited patient information R during the treatment process, that is, the similarity (distance) between the behavior matrix M and the expectation matrix EM. By calculating the Euler distance $\text{ED}(\text{SM}, M)$ of M and EM, and normalizing it to get the work target correlation P, and $P \epsilon [0, 1]$.

$$\text{ED}(\text{EM}, M) = \sqrt{(\text{EM} - M)(\text{EM} - M)^T},$$
$$P = 1 - \frac{\text{ED}(\text{EM}, M)}{\text{MAX}\,(\text{ED}(\text{EM}, M))}. \tag{16}$$

where $\text{MAX}\,(\text{ED}(\text{EM}, M))$ is the maximum possible distance between EM and M. Euclidean distance is used to calculate the similarity, which can reflect the absolute difference of individual values. It is suitable for the analysis of the difference between the numerical values of different dimensions. At the same time, the higher the matrix similarity P indicates the higher the work target relevance, the safer the access behavior.

Definition 5. Target achievement rate C. The target achievement rate describes the degree of achievement (approximate degree) of the actual treatment efficiency compared to the expected treatment efficiency. The formal definition is as follows:

$$C = \begin{cases} \dfrac{\rho_{\text{suc}}}{\rho_{\text{suc}}^*}, \rho_{\text{suc}} < \rho_{\text{suc}}^*, \\ 1, \rho_{\text{suc}} \ge \rho_{\text{suc}}^*. \end{cases} \tag{17}$$

ρ_{suc} is the diagnosis rate of the current medical records, and $\rho_{\text{suc}} = 1/i$, i is the number of expected targets, ρ_{sus}^* is the expected diagnosis rate, that is, the average diagnosis rate required to complete the treatment task. The higher the achievement rate, the completion degree the better, the higher the credibility of the access behavior, and $C \in [0, 1]$.

Let ω_P and ω_C be the weights of the work goal correlation P and the achievement rate C, respectively, and $\omega_P, \omega_C \in [0, 1]$, $\omega_P + \omega_C = 1$, the doctor's ith medical record trust degree is ReT_i, as follows:

$$\text{ReT}_i = \omega_P \bullet P_i + \omega_C \bullet C_i \tag{18}$$

After calculating ReT_i, add an evaluation tag to mark the

nature of the current record. When $\mathrm{ReT}_i \epsilon [0.9,1]$, mark it as a benign visit; when $\mathrm{ReT}_i \epsilon [0.8,0.9)$, mark as normal visit, when $\mathrm{ReT}_i \epsilon [0,0.8)$, mark as malicious visit. The evaluation label provides a judgment basis for the trust punishment strategy.

In order to increase the sensitivity and dynamics of the evaluation system, this paper uses a time decay function to perform a weighted average on the calculated medical record trust ReT_i to obtain the final average medical record trust value ReT as follows:

$$\mathrm{ReT} = \frac{1}{n}\sum_{i=1}^{n} \omega_i \cdot \mathrm{ReT}_i. \tag{19}$$

Divide the medical records in HIS into n time periods according to the timeline. Each time period may contain one or more medical records, and the same time period has the same weight ω, where ω_i is the weight of the ith time period, and the definition of ω_i as follows:

$$f(i) = 1 - \left(\frac{i}{n+1}\right)^{k+1} \quad k > 0, \tag{20}$$

$$\omega_i = \frac{f(i)}{\sum_{i=1}^{n-1} f(i)}. \tag{21}$$

$f(i)$ is the time decay function, n is the number of time nodes, and i is the current time period. In order to make the whole evaluation system pay more attention to the recent doctors' visit behavior dynamics and trends, and the medical records that are too old are only used as a certain reference, we choose $k > 0$ to make it appear to be attenuated over time The characteristics of acceleration, the selection of the specific k value can be flexibly changed according to requirements.

4.3.3. Evaluation of Doctors' Behavioral Reputation

Definition 6. Behavioral reputation BR. BR is the credit status of doctors' historical behavior from a macroperspective. If doctors can maintain good access behavior for a long time, BR will have a good accumulation. If malicious access behavior occurs, it will decrease, and the decline is greater than the increase, that is, it is easier to destroy reputation than to establish reputation.

Based on the literature [21, 34], this paper introduces the reputation penalty strategy to reflect the objective law of the slow increase and decrease of the reputation value in the real environment. The reputation evaluation algorithm is defined as

$$\mathrm{BR} = \begin{cases} \dfrac{\sum_{i=1}^{n} B_i}{\sum_{i=1}^{n} M_i + \sum_{i=1}^{n} B_i} - \dfrac{1}{1 + e^{1/\sum_{i=1}^{n} M_i}}, & \sum_{i=1}^{n} M_i \le \sum_{i=1}^{n} B_i, \\ 0, & \sum_{i=1}^{n} M_i > \sum_{i=1}^{n} B_i. \end{cases} \tag{22}$$

B_i is the number of benign visits and M_i is the number of malicious visits. Due to the existence of the penalty factor $1/(1 + e^{1/\sum_{i=1}^{n} M_i})$, once there is a malicious visit. Even if $\sum_{i=1}^{n} M_i > 0$, its visit reputation BR will be greatly reduced, which will increase the price paid by doctors for malicious visits. When malignant visits exceed benign visits, we consider its reputation value is zero.

Let ω_{ReT} and ω_{BR} be the preset weights of ReT and BR, respectively, $\omega_{\mathrm{HT}^*}, \omega_{\mathrm{BR}} \in [0, 1]$, and $\omega_{\mathrm{ReT}} + \omega_{\mathrm{BR}} = 1$, the final doctor's historical behavior trust HT algorithm is defined as

$$\mathrm{HT} = \omega_{\mathrm{ReT}} \cdot \mathrm{ReT} + \omega_{\mathrm{BR}} \cdot \mathrm{BR}. \tag{23}$$

5. Experiment and Analysis

5.1. Data Sources. Relying on the National Natural Science Foundation of China project "Medical Big Data Privacy and Security Risk Measurement and Privacy Protection in the Cloud Environment", this paper has completed related research experiments with the project partner of a third-class hospital in Kunming. All data are provided by the hospital, including 1360 tables with a total of 2,139,373 data. The experimental team extracted part of the data for research and analysis, mainly including data on the home page of medical records (37469), basic patient information (75705), and medical log (71453), medical order information (198780), error log (33336), employee information (3242), and login log (532). At the same time, the research team invited 10 experts from hospitals and universities to evaluate the weight of the trust evaluation index system established in this article. Among them, there are 3 directors and deputy directors of the clinical department of the hospital, 2 human resource management experts in the hospital, and 5 university experts in related research fields. All experts have more than five years of management or work experience, and have titles of associate senior or higher. The real data used in this article are all digitized data obtained after the data manager agrees and is processed with security technologies such as information desensitization.

5.2. Experiment Preparation

5.2.1. Establishment of Trust Evaluation System. The research team invited 10 experts to jointly complete the selection and empowerment of trust indicators, as follows.

(1) The weight calculation and consistency test of the first-level indicators. Table 4 shows the weights of the first-level indicators of doctor trust attributes

$\lambda_{\max} = 2$, $\mathrm{CI} = (\lambda_{\max} - n)/n - 1 = 0$; no consistency check is required.

(2) The weight calculation and consistency test of the second-level indicators. Tables 5 and 6 for the core competitiveness evaluation index weight and the interpersonal quality evaluation index weight

$\lambda_{\max} = 4.207$, $\mathrm{CI} = (\lambda_{\max} - n)/(n - 1) = 0.069$, $CR = 0.078 < 0.1$, pass the consistency test.

Table 4: First-level index weights of doctor trust attributes.

Trust evaluation index	T_1	T_2	w_{T_i}
Core competence (T_1)	1.000	2.000	0.667
Interpersonal quality (T_2)	0.5000	1.000	0.333

Table 5: Core competitiveness evaluation index weight.

Core competence (T_1)	t_{11}	t_{12}	t_{13}	t_{14}	$w_{t_{1i}}$
Academic degree (t_{11})	1.000	0.500	1.250	1.450	0.245
Working years (t_{12})	2.000	1.000	0.660	0.870	0.268
Quality of treatment (t_{13})	0.800	1.520	1.000	1.220	0.270
Tact (t_{14})	0.680	1.150	0.820	1.000	0.217

Table 6: Interpersonal quality evaluation index weight.

Interpersonal quality (T_2)	t_{21}	t_{22}	t_{23}	$w_{t_{2i}}$
Kindness (t_{21})	1.000	1.080	0.680	0.300
Communication skills (t_{22})	0.930	1.000	1.210	0.345
Doctor-patient relationship (t_{23})	1.470	0.830	1.000	0.355

$\lambda_{\max} = 3.050$, $CI = (\lambda_{\max} - n)/(n-1) = 0.025$, CR = 0.048 < 0.1, pass the consistency test.

Finally, the weight vector of the first level index is $W_T = \{0.667, 0.333\}$, and the weight vector of the second level index is $W_{T_1} = \{0.245, 0.268, 0.270, 0.217\}$, $W_{T_2} = \{0.300, 0.345, 0.355\}$. From Table 4, we find that compared with the interpersonal quality T_2, the doctor's trust is more dependent on its core competence T_1, which coincides with the research in the literature [35, 36] and also verifies the trust established in this article The rationality of the indicator system. $w_{t_{ij}}$ is the relative weight of the index t_{ij}. In order to show the direct influence of each trust index on the doctor's trust degree more intuitively, we define the direct weight $w_t^* = w_t \cdot w_T$, then the direct trust degree of the first-level trust index is as follows: $w_{t_{11}}^* = w_{t_{11}} \cdot w_{T_1}$=0.163, $w_{t_{12}}^* = w_{t_{12}} \cdot w_{T_1}$=0.179, $w_{t_{13}}^* = w_{t_{13}} \cdot w_{T_1}$=0.180, $w_{t_{14}}^* = w_{t_{14}} \cdot w_{T_1}$=0.145, $w_{t_{21}}^* = w_{t_{21}} \cdot w_{T_2}$=0.100, $w_{t_{22}}^* = w_{t_{22}} \cdot w_{T_2}$=0.115, and $w_{t_{23}}^* = w_{t_{23}} \cdot w_{T_2}$=0.118, The details are shown in Figure 4.

5.2.2. Role Attribute Trust Distribution. The research team randomly selected 60 doctors $d_1, d_2, \cdots, d_{60}$ from a third-class hospital in Kunming as sample doctors and evaluated the trust degree according to the index system of 5.1.1. We divided the trust evaluation level into 5 levels from low to high and adopts the arithmetic scoring method. The highest score for each indicator is 5.00 points, the lowest score is 1.00 points, with 0.5 as the smallest increment, and the highest is 5.00 points. After the gray statistics are normalized, the final character attributes are obtained: Trust value RT and RT $\in$ [0.00,1.00]. The final evaluation result distribution is shown in Figure 5.

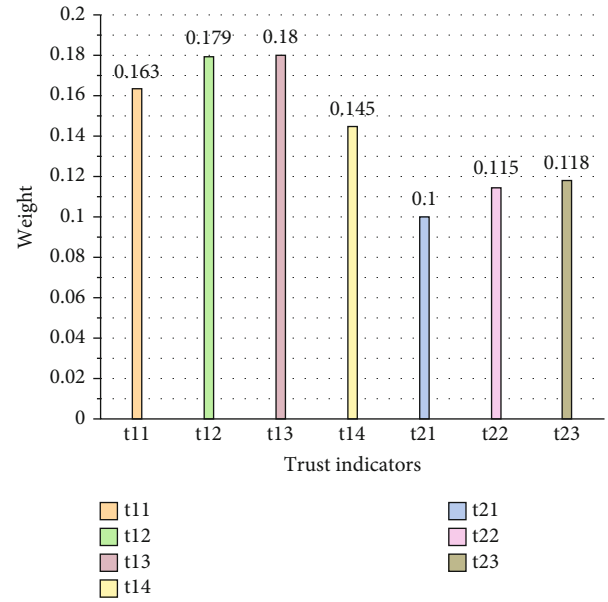

Figure 4: Direct weights of trust indicators.

As shown in Figure 6, the probability statistics of the doctor's trust evaluation data show that the relative frequency of the doctor's role attribute trust distribution decreases from 0.7 to the left and right and is concentrated in [0.7 – 0.8]. After fitting, it is found that it is similar to the Gaussian distribution of $X \sim N(0.76, 0.01)$.

5.3. Model Performance Analysis. This article consulted experts in related fields of universities and hospitals, and finally set the indicators as: $\omega_{RT} = 0.4$, $\omega_{HT} = 0.6$, $\omega_P = 0.4$ $\omega_C = 0.6$, and $k = 2$.

The dataset simulated in this paper includes 6000 historical visit records of 600 doctors randomly generated, each historical visit record contains several visits, and the visit records of doctors are divided into five time periods of $\{t_1, t_2, t_3, t_4, t_5\}$ according to the linear time order, and each time period contains 2 access records. According to the target achievement rate, target relevance, and role trust, 600 doctors are divided into honest doctor type @*A*, malicious doctor type @*B*, @*C*, and @*D*. The specific rules for generating various types of doctors are shown in Table 7.

When $C < 0.65$, the achievement rate is considered abnormal; otherwise, it is normal. In the dataset generated by the experimental simulation, RT is randomly generated in the interval [0-1] according to $X \sim N(0.75, 0.01)$.

5.3.1. Effectiveness Analysis. In this experiment, we mainly conduct a comprehensive trust evaluation of the simulated doctors, and compare whether the CT distinction between "honest doctors" and the three types of "malicious doctors" is obvious, and whether the group of doctors with the highest comprehensive trust score is mostly honest doctors. Whether most of the doctors with the lowest trust score are malicious doctors. According to the rules in Table 7, 600 doctors were randomly generated, the proportions of each type of doctor

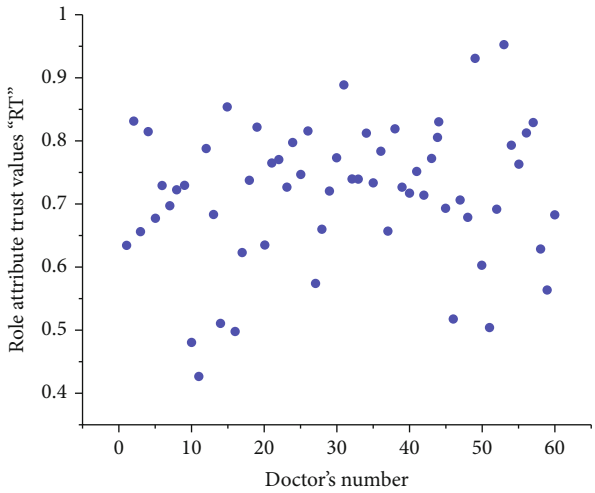

Figure 5: Distribution of doctor trust attributes.

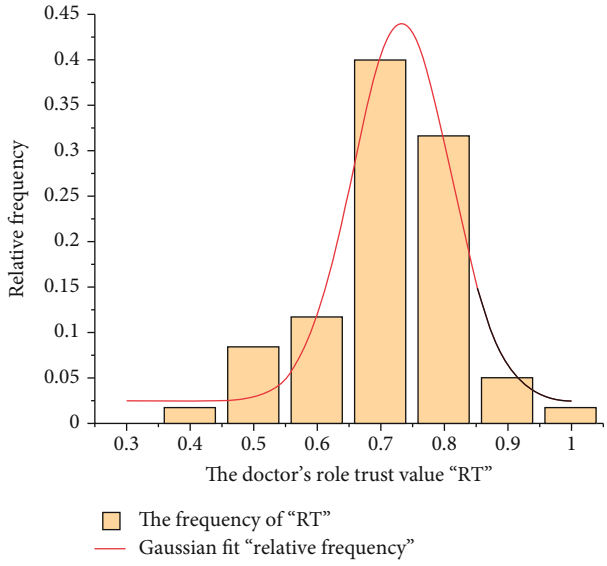

Figure 6: Probability distribution and fitting function of doctor's role attribute trust value.

were @A (85%), @B (5%),@C (5%), and @D (5%), specific experimental results, as shown in Figure 7.

In Figure 7, the average comprehensive trust of @A doctors is 1.2, 1.3, and 1.6 times that of @B, @C, and @D doctors, and the average comprehensive trust of "honest doctors" is 1.3 times that of "malicious doctors." It shows that the two types of doctors are clearly distinguishable, and the model in this paper is effective. According to Figure 8, in this experiment, the 20 doctors with the lowest trust score are all malicious doctors, and the accuracy rate of the top 50 doctors with the lowest trust score is also maintained at more than 90%.

5.3.2. Sensitivity Analysis. Sensitivity analysis mainly tests the sensitivity of the "traditional model" that uses the average weight distribution and the "this paper model" that uses the time decay function to dynamically distribute the weights to the development trend of "unstable doctors." In other words, based on the doctor's historical visit records and recent visit behavior characteristics, which model can more quickly discover and predict the doctor's future visit behavior trends? This experiment simulates the "unstable doctor" transformation process of @A ~ @D type, where the maximum sample interval $S_{\max} = 10$, and the doctor's initial comprehensive trust value CT = 1.0. We set each trust parameter of legal access behavior to 1.0, and each trust parameter of illegal access behavior to 0.6. The reason why the trust parameter is set at 0.6 for illegal access behavior is similar to that when the full score is 1, the passing line is 0.6. This is because it was found after several trials that this value can more accurately describe and predict the trend of doctors' future visits based on the doctor's historical visit records and recent visits behavior characteristics. The weight of the traditional model is $w_i^* = 0.1, i \in \{1, 2, \cdots, 10\}$, According to formulas (20) and (21), the time decay weight of the model in this paper is $w_i = [0.027, 0.048, 0.069, 0.087, 0.103, 0.116, 0.127, 0.136, 0.142, 0.145]$ where $i \in \{1, 2, \cdots, 10\}$.

The trust value of traditional medical records is recorded as ReT*, and the trust value of comprehensive medical records is recorded as ReT. The experimental results are shown in Table 8 and Figure 9.

Sensitivity analysis mainly tests the sensitivity of the model to the development trend of "change doctors," that is, whether it can more quickly discover and predict future visit behavior trends of the doctor based on the doctor's historical visit records and recent visit behavior characteristics. This experiment simulates the "changing doctor" transformation process of @A ~ @D type, where the maximum sample interval $S_{\max} = 10$, the doctor's initial comprehensive trust value CT = 1, the traditional average weight is w^*, and the traditional medical record trust value is ReT^*. The experimental results are shown in Table 8 and Figure 9.

In Figure 9, compared with the traditional algorithm using the average weight, the algorithm using the time decay function in this paper reduces the doctor's trust value more quickly under the continuous malicious visit behavior, so that the malicious behavior is found earlier. According to Table 7, when the doctor made the fourth malicious visit ($\mathrm{ReT}_4 = 0.78 < 0.80$), the algorithm in this paper has identified the behavior as a malicious visit, and the traditional algorithm until the sixth time ($\mathrm{ReT}_6^* = 0.76$) to identify the malicious visit behavior of the doctor. Therefore, under the same access behavior, the trust algorithm model adopted in this paper is more sensitive to malicious access behavior than the model using traditional algorithms.

5.3.3. Safety Analysis. Reputation evaluation is a security strategy generated by simulating interpersonal communication. The determination of reputation value is corrected through continuous interaction and feedback. The proposal of this idea makes up for the shortcomings of traditional security technology to a certain extent [37]. However, dynamic repair will also increase the risk of being "bleached attack" and make the reputation evaluation system invalid. This experiment mainly analyzes the ability of the trust

Table 7: Rules for generating simulation datasets.

Doctor type	Type code	Achievement rate, C	Target relevance, P	Role trust, RT
Honest doctor	@A	Normal	Normal	Gauss random
	@B	Normal	Abnormal	Gauss random
Malicious doctor	@C	Abnormal	Normal	Gauss random
	@D	Abnormal	Abnormal	Gauss random

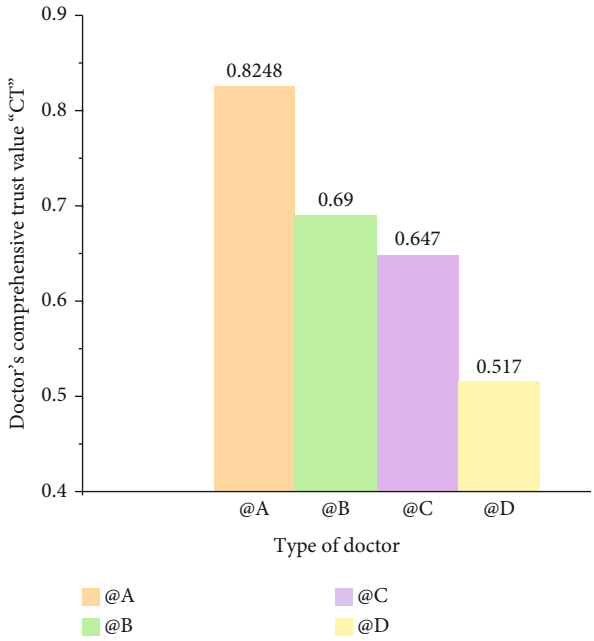

Figure 7: Comprehensive trust value of four types of doctors.

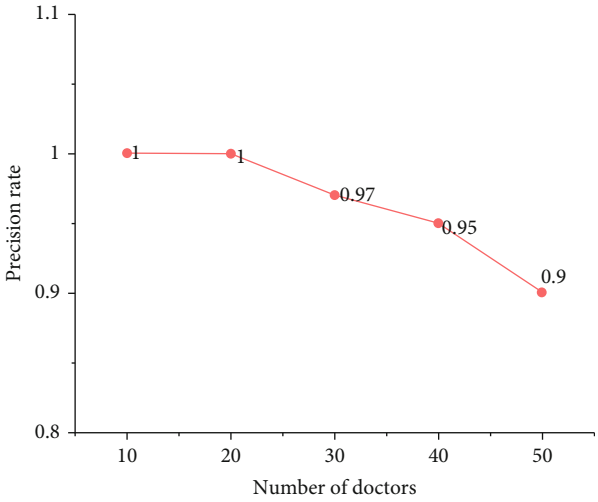

Figure 8: Trust evaluation efficiency.

algorithm in this paper to resist "bleaching attack" and compares it with the algorithm in literature [23].

In this experiment, $S_{max} = 200$, the doctor's initial medical record is $R = \{R_1, R_2, \cdots, R_{200}\}$, suppose the doctor's latest medical record R_{200} is marked as a malignant visit, and other

Table 8: Historical trust values of different visit times.

Number of visits	Medical records	P	C	Re T_i	ReT	ReT*
0	R1-R10	1.0	1.0	1.0	1.0	1.0
1	R2-R10	1.0	1.0	1.0	0.942	0.960
	R11	0.6	0.6	0.6		
2	R3-R10	1.0	1.0	1.0	0.885	0.920
	R11-R12	0.6	0.6	0.6		
3	R4-R10	1.0	1.0	1.0	0.831	0.880
	R11-R13	0.6	0.6	0.6		
4	R5-R10	1.0	1.0	1.0	0.780	0.840
	R11-R14	0.6	0.6	0.6		
5	R6-R10	1.0	1.0	1.0	0.733	0.800
	R11-R15	0.6	0.6	0.6		
.						
.						
.						
9	R10	1.0	1.0	1.0	0.6	0.6
	R11-R19	0.6	0.6	0.6		

visits are marked as normal visits. The experiment observes that the doctor's reputation value changes when performing a "bleaching attack" with a benign visit after a malicious visit. The number of benign visits increases from 0 to 200. The specific experimental results are shown in Figure 10.

In Figure 10, the algorithm in [23] with the continuous increase of benign visits, its trust value approaches 1, and finally almost completely covers the influence of past malicious visits on reputation. The algorithm used in this article adds a penalty factor to increase the impact of malicious visits on reputation. Even if there is only one malicious visit, the reputation will be reduced to about 0.73. Even if a large number of benign visits are followed up, it still cannot cover up the past. For the influence of malicious behavior on reputation, so compared with the literature [23], the reputation algorithm of this paper has stronger anti-bleaching attack ability. Literature [21] also uses the strategy of introducing a penalty factor to strengthen the algorithm's ability to resist bleaching attacks, but the fatal point is that the introduction of the penalty factor will cause permanent "damage" to the reputation, which may eventually cause the user's reputation to collapse. The evaluation model in this article uses the "queue" idea to avoid this situation.

In this experiment, $S_{max} = 200$, the initial sample set $R = \{R_1, R_2, \cdots, R_{200}\}$, after i times of updates, it becomes $R = \{R_{1+i}, R_{2+i}, \cdots, R_{200+i}\}$, when $i = S_{max}200$, the sample collection is all updated, and the medical record R_{200} is marked

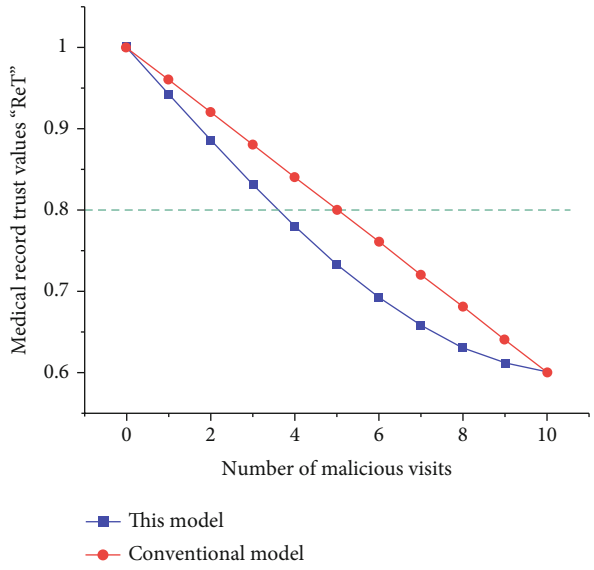

Figure 9: Trends in trust value of different malicious visits.

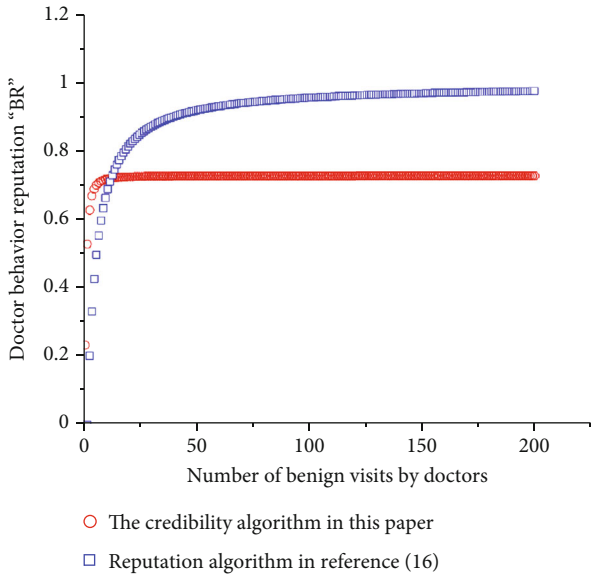

Figure 10: The trend of doctor's reputation value (benign visits increase).

as malicious. When the doctor performs 200 nonmalicious visits again, the evaluation sample $\{R_1, R_2, \cdots, R_{200}\}$ is updated to $\{R_{201}, R_{202}, \cdots, R_{400}\}$, and the malicious visit behavior is recycled out of the evaluation sample, that is, one malicious act of a doctor requires 200 nonmalicious visits to eliminate the impact. The price paid by doctors for malicious visits is related to the sample interval $S_{\max}$. The larger $S_{\max}$ is, the higher the price for malicious visits is. $S_{\max}$ can be flexibly selected according to needs. Therefore, the reputation algorithm in this article has higher antiwhitening ability and stronger flexibility.

Let 200 benign visits, the number of malicious visits increase from 0 to 200, and $S_{\max} \geq 400$ (that is, sample

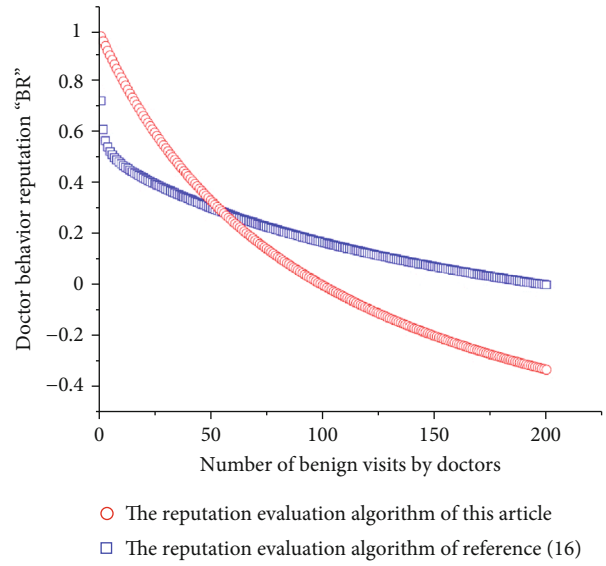

Figure 11: The trend of doctor's reputation value (malignant visits increase).

records do not need to be popped). The performance comparison of the reputation algorithm in this paper and the algorithm in literature [23] is shown in Figure 11.

In Figure 11, with the accumulation of malicious visits, the reputation value of literature [23] decreases slowly and is less sensitive to malicious visits, and the reputation value drops to negative as the number of malicious visits increases to about 100. The value continues to decline as the number of malicious visits increases. The credibility evaluation of this algorithm is obviously not logical and realistic. In comparison, the reputation algorithm in this paper quickly drops to a very low value (about 0.613) during the first few (2) malicious visits. When it drops to a certain value, the number of malicious visits increases, and the reputation value is always maintained at [0,1], which reflects the objective law of the sudden drop in reputation value, while ensuring the reasonableness of the reputation value.

6. Conclusion

The popularization of electronic medical records and the continuous improvement and development of HIS have made big data medical treatment a necessary trend in the development of medical informatization in the future. How to balance the advantages and disadvantages of medical informatization will also become a hot topic in future research. This paper proposes an access control model based on two-dimensional trust evaluation for medical big data. It conducts fine-grained trust evaluation on doctors from the two dimensions of role attributes and historical behavior and dynamically adjusts their access capabilities, thereby avoiding The doctor's malicious visit caused the leakage of patient information. This article uses real data and simulated data to conduct a series of comparative experiments. The experimental results show that the model is effective in suppressing malicious access behavior. The model's dynamics,

sensitivity, and resistance to bleaching attacks have been improved compared to other solutions.

In the future, we plan to study more complex cases of doctor-patient interaction and analyze and sort out a more complete and scientific evaluation index system for these complex situations. At the same time, this paper verifies the performance improvement of this model compared with other models in trust quantitative evaluation (implicit target) through experiments. Under normal circumstances, the improvement of implicit target performance will ultimately affect the performance of the displayed target. Therefore, we plan to prove the explicit target performance of the model through malicious behavior detection in real data. We also plan to refer to more advanced access control models and recent solutions commonly used in big data systems, and develop some hybrid access control models to handle the use, storage, communication, and operation of medical data.

Data Availability

The datasets used and/or analyzed during the current study are available from the authors on reasonable request.

Conflicts of Interest

The authors declare that they have no competing interests.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (Nos. 71972165 and 61763048) and Science and Technology Foundation of Yunnan Province (No. 202001AS070031).

References

[1] H. Chengyi and Z. Wu, "Privacy protection access control model for patient-oriented medical information systems," *Computer Applications and Software*, vol. 31, pp. 75–77, 2014.

[2] J. Andreu-Perez, C. C. Poon, R. D. Merrifield, S. T. Wong, and G. Z. Yang, "Big data for health," *IEEE Journal of Biomedical and Health Informatics*, vol. 19, no. 4, pp. 1193–1208, 2015.

[3] M. Chen, S. Mao, and Y. Liu, "Big data: a survey," *Mobile Networks and Applications*, vol. 19, no. 2, pp. 171–209, 2014.

[4] J. Luo, M. Wu, D. Gopukumar, and Y. Zhao, "Big data application in biomedical research and health care: a literature review," *Biomed Inform Insights*, vol. 8, pp. 1–10, 2016.

[5] G. Perera, A. Holbrook, L. Thabane, G. Foster, and D. J. Willison, "Views on health information sharing and privacy from primary care practices using electronic medical records," *International Journal of Medical Informatics*, vol. 80, no. 2, pp. 94–101, 2011.

[6] H. Zhen, L. Hao, Z. Min, and F. Dengguo, "Risk-adaptive access control model for medical big data," *Journal of Communications*, vol. 36, pp. 190–199, 2015.

[7] H. Xiaoxia, *On the Protection of Patient Information in Electronic Medicine*, Shandong University, 2018.

[8] D. Chen and H. Zhao, "Data security and privacy protection issues in cloud computing," in *2012 International Conference on Computer Science and Electronics Engineering*, pp. 647–651, Hangzhou, Zhejiang, China, 2012.

[9] A. Singh and K. Chatterjee, "Trust based access control model for securing electronic healthcare system," *Journal of Ambient Intelligence and Humanized Computing*, vol. 10, no. 11, pp. 4547–4565, 2019.

[10] T. Bhattasali, R. Chaki, N. Chaki, and K. Saeed, "An adaptation of context and trust aware workflow oriented access control for remote healthcare," *International Journal of Software Engineering and Knowledge Engineering*, vol. 28, no. 6, pp. 781–810, 2018.

[11] A. Singh and K. Chatterjee, "ITrust: identity and trust based access control model for healthcare system security," *Multimedia Tools and Applications*, vol. 78, no. 19, pp. 28309–28330, 2019.

[12] Y. Huang and K. Li, "Model of cloud computing oriented T-RBAC," *Application Research of Computers*, vol. 30, pp. 3735–3737, 2013.

[13] L. Zhang, A. Brodsky, and S. Jajodia, "Toward information sharing: benefit and risk access control (BARAC)," in *Seventh IEEE International Workshop on Policies for Distributed Systems and Networks (POLICY'06)*, pp. 45–53, London, ON, Canada, 2006.

[14] M. Gupta, F. Patwa, and R. Sandhu, "An attribute-based access control model for secure big data processing in Hadoop ecosystem," in *Proceedings of the Third ACM Workshop on Attribute-Based Access Control*, pp. 13–24, Tempe, AZ, USA, 2018.

[15] M. Gupta, F. Patwa, and R. Sandhu, *Object-Tagged RBAC Model for the Hadoop Ecosystem*, vol. 10359, Springer, Cham, 2017.

[16] A. K. Yadav, R. Ritika, and M. L. Garg, "SecHMS- A secure hybrid monitoring scheme for cloud data monitoring," *ICST Transactions on Scalable Information Systems*, vol. 8, article 166719, 2021.

[17] F. M. Awaysheh, M. Alazab, M. Gupta, T. F. Pena, and J. C. Cabaleiro, "Next-generation big data federation access control: a reference model," *Future Generation Computer Systems*, vol. 108, pp. 726–741, 2020.

[18] M. Wilikens, S. Feriti, A. Sanna, and M. Masera, "A context-related authorization and access control method based on RBAC," in *Proceedings of the seventh ACM symposium on Access control models and technologies*, pp. 117–124, Monterey, California, USA, 2002.

[19] Q. Wang and H. Jin, "Quantified risk-adaptive access control for patient privacy protection in health information systems," in *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security*, pp. 406–410, Hong Kong, China, 2011.

[20] E. Dong, *Construction of Patient Trust Evaluation Index System Based on Medical Quality Management and Related Research*, Shanghai Jiaotong University, 2012.

[21] Z. Wenfang, G. Dong, X. Wang, and W. Wu, "Task-role-based access control model based on multi-step dynamic trust evaluation," *Computer Integrated Manufacturing System*, vol. 24, pp. 1983–1995, 2018.

[22] S. Chakraborty and I. Ray, "TrustBAC: integrating trust relationships into the RBAC model for access control in open systems," in *Proceedings of the eleventh ACM symposium on Access control models and technologies*, pp. 49–58, Lake Tahoe, California, USA, 2006.

[23] L. Hongyue, Y. Junzhi, and J. Ma, "A fine-grained RBAC access control model framework based on credibility," *Journal on Communications*, vol. 30, pp. 51–57, 2009.

[24] R. Banyal, V. Jain, and P. Jain, "Dynamic trust based access control framework for securing multi-cloud environment," in *Proceedings of the 2014 International Conference on Information and Communication Technology for Competitive Strategies*, pp. 1–8, Udaipur, Rajasthan, India, 2014.

[25] R. Yang and X. Yu, "Research on building the credibility evaluation's indicator system of cloud end user's behavior," in *2017 ieee 3rd international conference on big data security on cloud (bigdatasecurity), ieee international conference on high performance and smart computing (hpsc), and ieee international conference on intelligent data and security (ids)*, pp. 43–47, Beijing, China, 2017.

[26] L. Yuanbing, Z. Wenfang, and X. Wang, "Access control scheme based on multi-attribute fuzzy trust evaluation in cloud manufacturing environment," *Computer Integrated Manufacturing System*, vol. 24, pp. 321–330, 2018.

[27] D. K. Vawdrey, T. L. Sundelin, K. E. Seamons, and C. D. Knutson, "Trust negotiation for authentication and authorization in healthcare information systems," in *Proceedings of the 25th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (IEEE Cat. No.03CH37439)*, vol. 2, pp. 1406–1409, Cancun, Mexico, 2003.

[28] A. Boukerche and Y. Ren, "A secure mobile healthcare system using trust-based multicast scheme," *IEEE Journal on Selected Areas in Communications*, vol. 27, no. 4, pp. 387–399, 2009.

[29] C. Dong and N. Dulay, "Privacy preserving trust negotiation for pervasive Healthcare," in *2006 Pervasive Health Conference and Workshops*, pp. 1–9, Innsbruck, Austria, 2006.

[30] A. Singh and K. Chatterjee, "An adaptive mutual trust based access control model for electronic healthcare system," *Journal of Ambient Intelligence and Humanized Computing*, vol. 11, no. 5, article 1240, pp. 2117–2136, 2020.

[31] T. L. Saaty, "What is the analytic hierarchy process?," in *Mathematical models for decision support*, pp. 109–121, Springer, Berlin, Heidelberg, 1988.

[32] T. L. Saaty, "Decision making with the analytic hierarchy process," *International journal of services sciences*, vol. 1, no. 1, pp. 83–98, 2008.

[33] T. L. Saaty, *Fundamentals of Decision Making and Priority Theory with the Analytic Hierarchy Process*, RWS Publications, 2000.

[34] T.-Y. Chen, Y.-M. Chen, C.-B. Wang, H.-C. Chu, and H. Yang, "Secure resource sharing on cross-organization collaboration using a novel trust method," *Robotics and Computer-Integrated Manufacturing*, vol. 23, no. 4, pp. 421–435, 2007.

[35] S. D. Pearson and L. H. Raeke, "Patients' trust in physicians: many theories, few measures, and little data," *Journal of General Internal Medicine*, vol. 15, no. 7, pp. 509–513, 2000.

[36] S. M. Bachinger, A. M. Kolk, and E. M. Smets, "Patients' trust in their physician–psychometric properties of the Dutch version of the "Wake Forest Physician Trust Scale"," *Patient Education and Counseling*, vol. 76, no. 1, pp. 126–131, 2009.

[37] S. Xiaoyin, G. Wu, Y. Dong, and Y. Ping, "A recommendation-based reputation system initialization strategy," *Journal of Southeast University (Natural Science Edition)*, vol. 40, pp. 41–46, 2010.