frontiers in Public Health

ORIGINAL RESEARCH
published: 10 September 2021
doi: 10.3389/fpubh.2021.718594

An Intelligent Control Model of Credit Line Computing in Intelligence Health-Care Systems

Rong Jiang[1,2,3], *Wenxuan Wu*[1,2,3,4], *Yimin Yu*[1,2,3,4]* *and Feng Ma*[4]

[1] *Institute of Intelligence Applications, 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] *School of Information, Yunnan University of Finance and Economics, Kunming, China*

OPEN ACCESS

Edited by:
Ying Li,
Zhejiang University, China

Reviewed by:
Qiang Hu,
Qingdao University of Science and Technology, China
Xianwei Li,
Waseda University, Japan
Donghui Yang,
Southeast University, China

****Correspondence:***
Yimin Yu
yuyimin@ynufe.edu.cn

Specialty section:
This article was submitted to Digital Public Health, a section of the journal Frontiers in Public Health

Received: *01 June 2021*
Accepted: *31 July 2021*
Published: *10 September 2021*

Citation:
Jiang R, Wu W, Yu Y and Ma F (2021) An Intelligent Control Model of Credit Line Computing in Intelligence Health-Care Systems. Front. Public Health 9:718594. doi: 10.3389/fpubh.2021.718594

Technologies such as machine learning and artificial intelligence have brought about a tremendous change to biomedical computing and intelligence health care. As a principal component of the intelligence healthcare system, the hospital information system (HIS) has provided great convenience to hospitals and patients, but incidents of leaking private information of patients through HIS occasionally occur at times. Therefore, it is necessary to properly control excessive access behavior. To reduce the risk of patient privacy leakage when medical data are accessed, this article proposes a dynamic permission intelligent access control model that introduces credit line calculation. According to the target given by the doctor in HIS and the actual access record, the International Classification of Diseases (ICD)-10 code is used to describe the degree of correlation, and the rationality of the access is formally described by a mathematical formula. The concept of intelligence healthcare credit lines is redefined with relevance and time Windows. The access control policy matches the corresponding credit limit and credit interval according to the authorization rules to achieve the purpose of intelligent control. Finally, with the actual data provided by a Grade-III Level-A hospital in Kunming, the program code is written through machine learning and biomedical computing-related technologies to complete the experimental test. The experiment proves that the intelligent access control model based on credit computing proposed in this study can play a role in protecting the privacy of patients to a certain extent.

Keywords: machine learning, biomedical computing, intelligence healthcare, privacy security, intelligent access control, credit line

INTRODUCTION

Medical big data (1) is a branch of big data in the field of biomedicine. It refers to the data related to life, health, and medical care generated in activities related to human health, mainly from intelligent medical systems such as clinical data, hospital, operation, biomedical research, disease prevention and control, health protection and food safety, public health and health management data, health care and other aspects (2). In these massive amounts of data, there are opportunities. If the data generated by smart medical care can be flexibly called after biomedical calculations, data pressure can be converted into data advantage (3, 4).

In terms of biomedicine, individual users have become an important source of data. The private information generated by smart medical treatment often means unspeakable pain for individuals. The leakage of such negative information has become a huge hidden danger in the era of big data (5). In the past, most patients maintained their personality and dignity through self-forgetting and the privacy of medical institutions (6). Nowadays, the ubiquitous smart medical equipment and cloud storage and cloud computing functions, such as placing users in a transparent glass room. Our every move may be recorded, and the electronic health records generated by the widely used smart medical system and smart medical equipment make it difficult for patients to hide their privacy. According to a security report released by Trust wave, more than 90% of the investigators believe that there are more and more cyberattacks against the medical field, but the budget for protecting sensitive patient information is <10% (7). Once the criminals steal medical data, they can easily learn the name, home address, contact information, test report, diagnosis results, and even medical insurance and other important information of the patient, and use this to falsify the data to defraud or purchase medical equipment. Therefore, the consequences of data theft in the medical field are very serious. More than two million people in the United States will become victims each year. The loss caused by this is as high as $13,500, and it will take hundreds of hours to solve this problem. In 2015, the social security system became the hardest hit area for personal information leakage, etc. (8). These incidents seriously violated the privacy and legal rights of users. At present, both the public and the government have begun to pay attention to personal privacy issues in medicine (9). In the United States, electronic health data are also being prepared for an online transformation. Dosia (a non-profit coalition of major employers), Google Health, Microsoft Health Vault, and other network services are driving this transformation. These services are seeking expanded role in the United States health-care system that values 21,000 dollars (10).

With China's accession to the WTO and the acceleration of social information, whether it has a fully functional intelligent medical system, it has become an important indicator to measure the comprehensive strength of a hospital (11, 12). A perfect hospital information system (HIS) includes outpatient management, hospitalization management, drug management, multiple subsystems, such as electronic medical records and financial management. The high integration between the various subsystems improves the overall operating efficiency of the hospital, improves the medical environment of the patient, and at the same time provides data-driven support for the management of hospital, clinical, etc. The electronic medical record system (13) includes the electronic medical record of the doctor and nurse. The main function is to save the medical records of the patients electronically. It not only includes the medication information of the patient, but also includes the treatment record, laboratory and examination records, and other information of the patient. The doctor is giving the past medical records and medical history of the patient during treatment. It can more accurately analyze the condition of the patient and treat the patient (7). However, due to the use of HIS, doctors can access a large amount of medical information, and the resulting medical problem of privacy leakage is also very tricky. When the system security and data security are not guaranteed, the intelligent medical system is fragile, which will not only cause great troubles for medical work, but also greatly reduce the prestige of the intelligent medical system (14).

Given the medical privacy leakage risk arising from the widespread use of intelligent medical systems today, this study proposes an access control model based on credit line calculations for intelligent medical systems. In this model, when doctors use the intelligent medical system to diagnose patients, they use historical records to calculate credit lines, and dynamically restrict doctors' access rights based on their credit capabilities. Don't give unnecessary permissions, and will not affect the normal work of doctors, try to comply with the A principle (15). The main steps of model realization are as follows:

(1) Through similarity function calculation, the results obtained by the mathematical method can be used to describe whether the inquiring behavior of the doctor is reasonable.
(2) The appropriate weight calculation method is used to obtain the weight value so that the unreasonable behavior of the doctor is easy to lead to the decline of the credit limit, but the reasonable behavior of the doctor will not affect his trust limit.
(3) According to the credit limit of the user, match the corresponding trust interval to achieve the ability to limit the access authority of the user. Doctors with a high credit limit will become larger and larger. On the contrary, doctors with a low credit limit will become smaller and smaller, until it is lower than the credit line threshold, and the visit is forbidden. In the existing model, doctors select medical records based on randomly assigned work goals, or medical records are selected based on the work goals selected by the doctors themselves, and this study defines that the doctors may not necessarily choose an honest work goal based on the preliminary examination information of the patient. In addition, the doctor will give a more accurate final diagnosis only after checking the medical records. The model can properly describe the real diagnosis process of the doctor, and it is more in line with the actual situation.

The contributions of this study are as follows:

1. Some contents have been added to the doctor behavior model in the study (16), which improves the performance of the model in screening curious doctors.
2. In a relatively mature intelligent medical system, the concept of the credit line is introduced as the carrier of medical trust computing.
3. After comparison, more appropriate trust calculation and weight calculation methods are selected to achieve the effect of using historical records to restrain the behavior of doctors and reduce the risk of privacy disclosure in the medical field.

RELATED WORKS

If divided by authorization strategy, the access control model can be divided into the following: traditional access control model (DAC/MAC), role-based access control (RBAC) model (17), task and workflow-based access control (TBAC) model (18), task-based and role-based access control (TRBAC) model, etc. (19). RBAC model permissions are associated with roles, and users become members of corresponding roles, which greatly simplifies the management of permissions. However, the RBAC model cannot be directly used for more complex forms of access control (20). Goyal et al. (21) proposed an attribute-based mechanism to protect data and avoid setting data owner rules. However, the main disadvantage of using attribute-based methods is that it will bring a high workload to the user side. For most ordinary users, with limited knowledge of rules or strategy design, creating a complex data access mechanism in a medical environment is an arduous task (22). The workload brought by traditional access

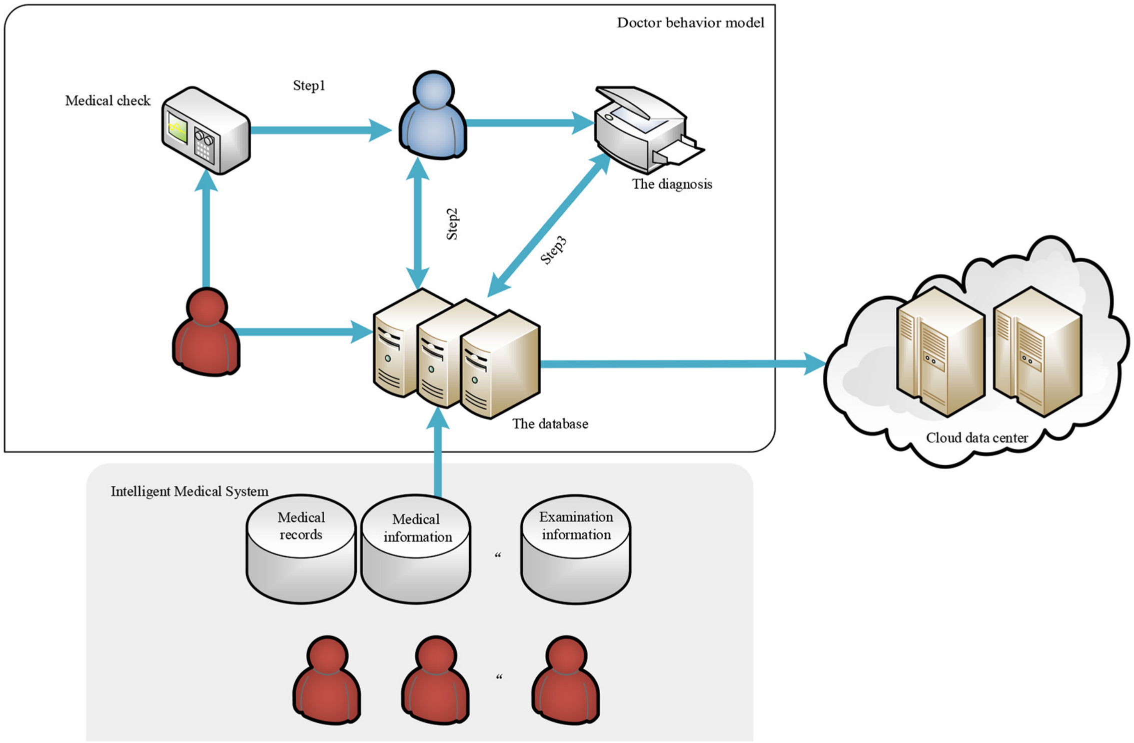

FIGURE 1 | Doctor behavior model.

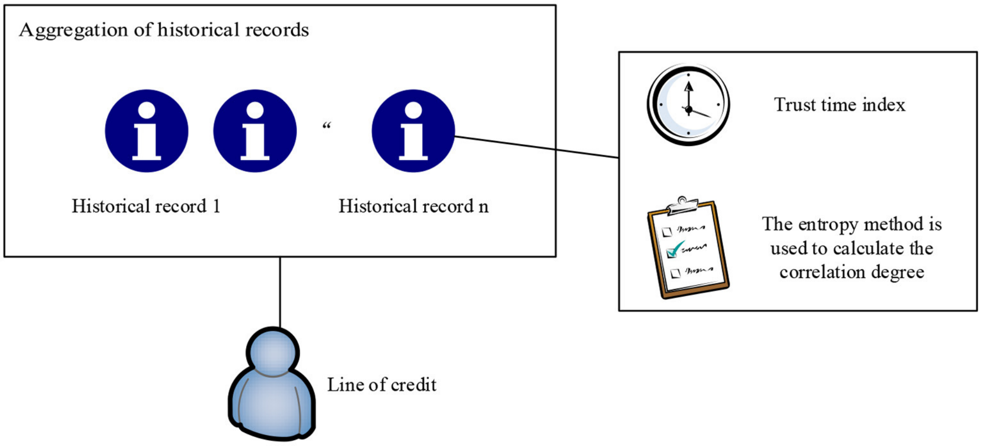
Aggregation of historical records
“
Historical record 1
Historical record n
Trust time index
The entropy method is used to calculate the correlation degree
Line of credit

FIGURE 2 | Trust calculation process.

control obviously cannot adapt to the situation of massive data in the context of big data.

Health and medical big data are important basic strategic resources of the country. Traditional database achieves security and privacy protection through data granularity-based security control, but the operation of big data still lacks effective security protection measures (23). The realization technology of medical big data information security includes access control and password technology. Data privacy implementation technologies include obfuscation, anonymity, differential privacy, and encryption (16). At present, the prominent problems in the use of HIS medical data mainly include the following:

(a) Security issues: dynamic permissions are granted. The existing medical information system does not consider the wishes of patients, and the scope of medical data that doctors can access is not detailed enough. According to the actual needs of doctors, there is little research on medical information systems that dynamically grant data access rights to achieve fine-grained data access.
(b) Data sharing issues: Doctors and researchers have strict restrictions when accessing and sharing medical data (24).

The important issue studied in this study is access control, with the focus on protecting information from unauthorized access (25). Wang et al. (26) designed a secure authentication algorithm to limit the access rights of access objects in the electronic medical record (EMR) system. Zhu et al. proposed a user-friendly, easy-to-manage, attribute-based access control (ABAC) for cloud storage services in 2015. This mechanism defines the priority of attributes and refines the granularity of data access control in the cloud environment (27). Liu et al. (28) is based on the trust-based access control model, which combines dynamic hierarchical fuzzy systems with trust evaluation, layered the attributes related to trust in the cloud manufacturing environment, and proposed a multi-attribute fuzzy trust evaluation access control scheme. Gao (29) built a flexible dynamic access control model to make up for the lack of static policies, making the original role, the static authorization access of permissions is transformed into a model that can dynamically authorize users. Zhang and Zhou (30) to solve the problems of access resources insufficient flexibility and preset allocation of permissions in the traditional role-based access control system, improved compatibility of access control, refine the granularity of access control, and propose a dynamic multilevel access control model based on trust. The static role and dynamic trust degree of the user obtain the corresponding authority authorization (31). Based on the traditional free access control (DAC) and RBAC model, a context-sensitive access control method is proposed, which strictly follows regulatory and technical standards in the health-care field to ensure authorized access (32). The literature found that existing symmetric and asymmetric encryption technologies have complex key management and certificate management problems. In response

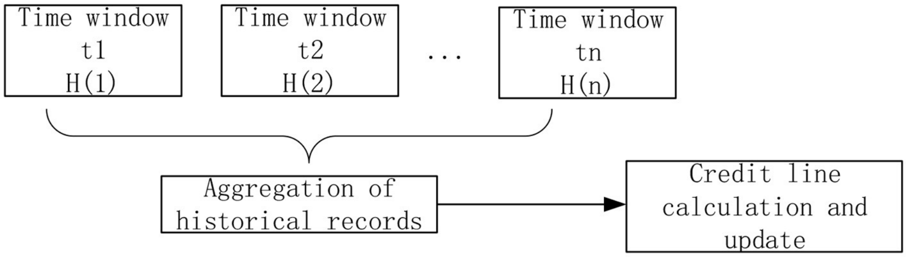

FIGURE 3 | History aggregation.

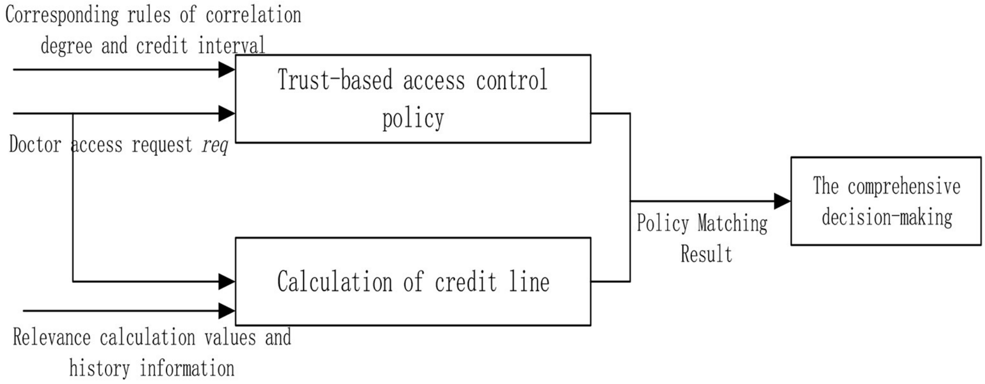
Corresponding rules of correlation
degree and credit interval
Trust-based access control
policy
Doctor access request *req*
Policy Matching
Result
The comprehensive
decision-making
Calculation of credit line
Relevance calculation values and
history information

FIGURE 4 | Access control scheme.

to these problems, the policy-based access control (PBAC) model and the purpose of joining conditions are proposed. IBE encryption technology medical data can access control scheme. Yang et al. (33) proposed a privacy protection medical big data system with adaptive access control. Through a new dual access control mechanism, the mechanism has adaptive capabilities for both normal and emergency medical data access. In summary, although various access control models have been expanded by previous researchers, yet studies on trust computing and access control models in the field of intelligent medical research are inadequate (34). The authorization method for access control in the process of diagnosis by doctors and treatment is relatively simple and restrictive. The problem of insufficient binding still exists.

Therefore, it is more necessary to explore a dynamic trust computing method and access control scheme, which are more suitable for specific occasions of medical access, and dynamically adjust the permissions of doctors to access medical resources through the results of trust computing, to improve the privacy protection performance of the model.

MODEL DESIGN

Based on the research of a large number of existing intelligent medical systems (35), this section presents the following behavior model which is more suitable for the actual situation. Taking the process of diagnosis by doctors and treatment of patients as the research object, the diagnosis and treatment behavior of doctors is abstracted into a model from the three aspects of examination information of doctors, access of doctors to medical data, and the diagnosis results are given. Then, the definition of credit limit, correlation calculation, and weight determination method are given.

Doctor Behavior Model

This is shown in **Figure 1**, for the diagnosis and treatment process of each patient, we call it a task. In the task, the diagnosis by doctor and treatment steps are generally the following: first browse the basic information of the patient, such as name, age, and past medical history. If the patient has a medical history in the hospital, the doctor can check the past examination items and results of the patient through the HIS database. Then, the patient will receive new test results according to the arrangement of the doctor, whose arrangement is also stored in the HIS database. The doctor can view the test results of the patient and certain related medical records (such as medical imaging data of other similarly diagnosed patients in the database, etc.) to obtain the final diagnosis for the patient. The medical data in the HIS database that doctors can view involve some sensitive information about the patient, but considering moral factors and the cost of leaks, hypothetical model doctors in China will not disclose any information about their patients. Based on the

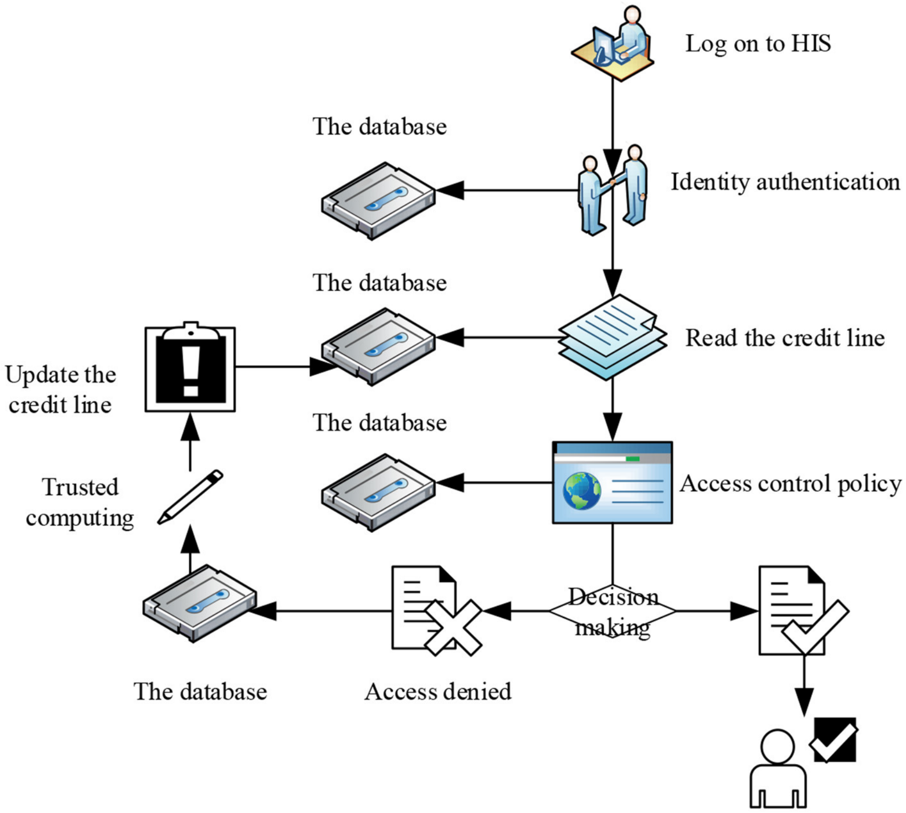

FIGURE 5 | Access control flow chart.

above behavior model, the behavior of privacy leakage of curious doctors will occur in the following three steps:

Step 1. The correlation between the examination information of the patient and the initial diagnosis given by the doctor is low. For example, the results of the examination of a patient can directly indicate that the patient is unlikely to have an infectious disease. However, the doctor still gave a preliminary diagnosis that the patient may have an infectious disease, and then consulted the relevant medical records of the patient with infectious disease based on the false preliminary diagnosis.
Step 2. Suppose that the doctor gave a correct preliminary diagnosis consistent with the examination information in Step 1, but inquired about unnecessary medical records when accessing the medical records based on the preliminary diagnosis.
Step 3. Assume that the doctor is operating normally in Step 1 and Step 2, but the final diagnosis has a low correlation with the medical records queried. It is suspected that the doctor had accessed unnecessary medical records.

Give the formal description of the symbol as follows, and abstract the process:

E: A collection of examination information;
P: A collection of primary diagnoses;
F: A collection of final diagnoses;
R: A collection of medical records.

$S_1 : E, P \rightarrow [0, 1]$: Define the correlation function between inspection information and preliminary diagnosis, $e \in E, p \in P$, where the return value of the function reflects the degree of correlation between the two in a certain diagnosis and treatment process.
$S_2 : P, R \rightarrow [0, 1]$: Define the correlation function between the initial diagnosis and medical records, $p \in P, r \in R$, where the return value of the function reflects the degree of correlation between the two in a certain diagnosis and treatment process.
$S_3 : R, F \rightarrow [0, 1]$: Define the correlation function between medical records and the final diagnosis, $r \in R, f \in F$, where the return value of the function reflects the degree of correlation between the two in a certain diagnosis and treatment process.

Trust Attribute System

The existing trust system for access control is relatively single, usually divided into direct trust and indirect trust. In the context of diagnosis and treatment by doctors, this trust model cannot accurately assess the credibility of behavior of doctors. Doctors have extensive access to patients and medical records in intelligent health-care systems, but there is a lack of effective direct trust between each doctor or between patients and other doctors (who do not diagnose themselves). According to the behavioral characteristics of diagnosis and treatment by doctors and the particularity of the structure of medical resource system, indirect trust is not considered in the trust attribute, but only the historical visit records of doctors will directly affect their credit line.

The concept of credit originates from the financial field and refers to the funds provided by banks to non-financial users, including but not limited to various businesses, such as loans. The credit line means the highest credit value given to users by the bank after calculation and evaluation during the credit period.

This study introduces the concept of credit line in the intelligent medical system, and redefines it as a comprehensive evaluation of the history records, access behavior, and other factors of medical information system, and calculates and grants credit line of the doctor user for overdraft use. The credit limit is calculated by reading the history of the doctor through HIS. The continuous integrity behavior record of the doctor can help increase the credit limit, and high-risk behaviors will lead to a reduction in the credit limit, thereby realizing dynamic access control to medical data. The history record includes two sub attributes of the trust time window and operational relevance. This is shown in **Figure 2**.

Correlation Calculation

In the intelligent medical system, doctors use electronic medical records to record the medical treatment of patients during the medical treatment process. This study introduces the International Classification of Diseases (ICD) as the code used by doctors in the diagnosis of electronic medical records. Suppose a certain disease in the electronic medical record is represented by an ICD code. Afterward, you can use the element group to write $a_1, a_2, a_3, ..., a_n$, the elements representing the disease at each location are divided into different subcategories according to the ICD code and expressed as $a_{i1}, a_{i2}, a_{i3}, ..., a_{in}$, where n represents the number of subcategories of the disease. To calculate the similarity, prepare to construct the initial judgment matrix EQ from the diseases in the medical records as follows:

$$EQ = \begin{Bmatrix} a_{11} & \ldots & a_{1n} \\ \ldots & \ldots & \ldots \\ a_{n1} & \ldots & a_{nn} \end{Bmatrix} \tag{1}$$

The three steps involved in diagnosis process by a doctor have different risks of privacy leakage. This section focuses on the calculation method of the correlation function. There are many methods to measure similarity (36), and the distance measurement is Minkowski distance, Euclidean distance, Manhattan distance, Hamming distance, etc. Commonly used similarity coefficients include cosine similarity, Pearson correlation coefficient, Jaccard correlation coefficient, etc. The traditional methods for measuring the similarity of two individuals are commonly used. Cosine similarity is defined as follows: regarding user information as an n-dimensional vector,

TABLE 1 | Correlation degree—credit interval rules.

	Correlation	The line of credit is in the range
1	0.8	$t_3 < t \leq t_4$
2	0.6	$t_2 < t \leq t_3$
3	0.4	$t_1 < t \leq t_2$
4	0.2	$t_0 < t \leq t_1$

the similarity is calculated as the cosine of the angle between the vectors. The similarity between individual i and j is recorded as shown:

$$\mathrm{sim}\left(i,j\right)=\cos\left(\vec{i},\vec{j}\right)=\frac{\vec{i}\cdot\vec{j}}{\left\|\vec{i}\right\|*\left\|\vec{j}\right\|} \tag{2}$$

$\vec{i}\cdot\vec{j}$ is the inner product and $\left\|\vec{i}\right\|*\left\|\vec{j}\right\|$ is the vector product.

In addition to cosine similarity, there is also correlation similarity. The similarity is measured by calculating the correlation coefficient between i and j of the item. Determine the common user set U of i and j, and the correlation similarity is defined as follows:

$$\mathrm{sim}\left(i,j\right)=\frac{\sum_{u\in U}\left(R_{ui}-R_i\right)\left(R_{uj}-R_j\right)}{\sqrt{\sum_{u\in U}\left(R_{ui}-R_i\right)^2}\sqrt{\sum_{u\in U}\left(R_{uj}-R_j\right)^2}} \tag{3}$$

The similarity is obtained by using cosine or correlation similarity, because the medical data category base is relatively large, and the data are dense, and the wrong conclusion with high similarity is obtained. When calculating the similarity, the Jaccard similarity coefficient is introduced to calculate the privacy leakage risk of the doctor in each step of the diagnosis process. The Jaccard similarity coefficient is also called the Jaccard index, which is used to compare the similarity and difference statistics of a limited sample set (37). Assume that sets I and F are the

TABLE 2 | Expert opinion weights.

	α	β	γ
Expert 1	0.6	0.2	0.2
Expert 2	0.3	0.6	0.1
Expert 3	0.5	0.3	0.2
…	…	…	…
Expert 9	0.4	0.3	0.3
Expert 10	0.2	0.3	0.5
MSD calculate	0.49	0.16	0.35

TABLE 3 | The results of doctors were judged by maximum score deviation (MSD) weights.

		Expert 3			**Expert 10**			**MSD**		
		Step 1	**Step 2**	**Step 3**	**Step 1**	**Step 2**	**Step 3**	**Step 1**	**Step 2**	**Step 3**
Special access	1		○			×			○	
	2		•			×			○	
Malicious access	1	○			•			○		
	2		○			○			○	
	3			•			○			○

•, Unable to determine; ○, right; ×, false.

TABLE 4 | Changes of historical aggregate values of doctors.

Doctor	**CT(1)**	**CT(2)**	**CT(3)**	**CT(4)**	**CT(5)**	**CT(6)**	**CT(7)**	**CT(8)**
Honest doctor	0.66	0.57	0.62	0.59	0.67	0.63	0.60	0.59
Special doctor	0.63	0.60	0.58	0.56	0.64	0.51	0.61	0.56
Curious doctor	0.51	0.43	0.57	0.64	0.66	0.67	0.58	0.47

TABLE 5 | The variation of the mean value of credit line with α.

Doctor	**Δ**	**α = 0.95**	**Δ**	**α = 0.5**	**Δ**	**α = 0.2**	**<Δ**
Honest doctor	0.16	0.596	0.11	0.604	0.12	0.583	0.13
Special doctor	0.31	0.557	0.12	0.585	0.14	0.602	0.19
Curious doctor	0.34	0.531	0.26	0.538	0.17	0.551	0.25

initial diagnosis and the final diagnosis is described using ICD codes. Each code contains n public attributes, which indicate the category and subcategory of the disease. Each attribute in the code consists of a number or letter. To facilitate the calculation, the number will be represented by the set of 0 and 1. The Jaccard index can be written as J (I, F). The definition of the Jaccard index is as follows (38):

$$J\,(I,F) = \frac{I\bigcap F}{I\bigcup F} \tag{4}$$

Define that when I=F=∅, J(I, F) = 1, the value range is [0,1], the larger the J value, the greater the similarity between the two samples. From this, the Jaccard distance can be obtained, and dJ (I, F) is used to represent the difference between the two samples:

$$\mathrm{d}_J\,(I,F) = 1 - J\,(I,F) = \frac{\left|I\bigcup F\right| - \left|I\bigcap F\right|}{\left|I\bigcup F\right|} \tag{5}$$

Taking the stomatology department as an example, suppose that the initial diagnosis given by a doctor is periodontitis. Define M11 as the number of ones in both I and F; M01 is the number of attributes of F that are 1 when the attribute of the set I is 0; M10 is the number of attributes of F in the set I that is 0 when the attribute is 1; M11 is the number of attributes of the set I and F that are 1. According to the above assumptions, the calculation method of Jaccard index and Jaccard coefficient can be obtained as follows:

$$M_{11} + M_{01} + M_{10} + M_{00} = \mathrm{n} \tag{6}$$

$$J = \frac{M_{11}}{M_{11} + M_{01} + M_{10}} \tag{7}$$

$$\mathrm{d}_J = \frac{M_{01} + M_{10}}{M_{11} + M_{01} + M_{10}} \tag{8}$$

According to the analysis of the above doctor behavior part, the doctor can directly contact the medical data of the non-attending patient during the diagnosis process, which is a high-risk reason for privacy leakage. To avoid a single error in the similarity calculation, cross-entropy is then used (39) to introduce the calculation of the similarity between two random variables.

Entropy is the expected value of the amount of information (40). Assuming that there is a random variable x with a value range of set X, its probability distribution function can be expressed as $\mathrm{p}\,(x) = \Pr\,(X = x)\,, x \in X$, and defines the amount of information as $I\,(x_1) = -\lg\left(p\,(x_1)\right)$, the greater the probability of an event, the more $p\,(x_1)$ larger, the smaller the amount of information it carries (41). In the extreme case $p\,(x_1) = 1$, the amount of information is equal to zero, which means that when the probability of an event happening is 100%, then the occurrence of this event will not introduce too much information. When we know the amount of information to measure the uncertainty of the occurrence of an event, we can calculate the expectation $(E\,[I\,(x)])$ for the additional information brought by all possible results, and the entropy can be defined as follows:

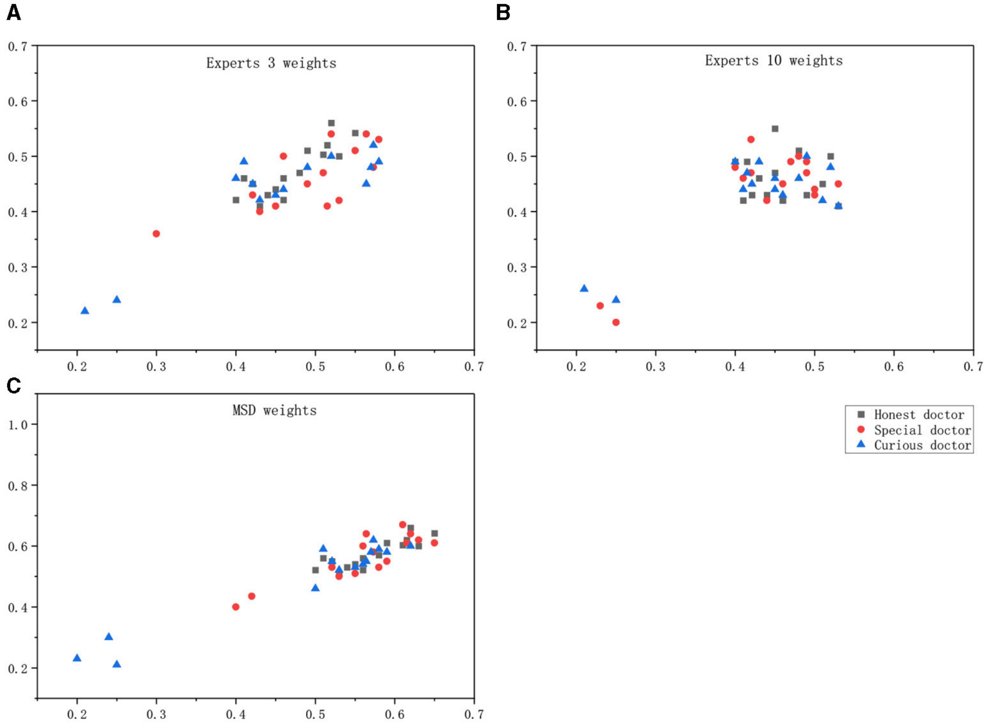

FIGURE 6 | Maximum score deviation (MSD) weight differentiating doctor effect. **(A)** Experts 3 weights, **(B)** Experts 10 weights, **(C)** MSD weights.

$$H(X) = Ep\left[\lg p(x)\right] = -\sum x \in Xp(x)\lg p(x) \tag{9}$$

According to the diseases and symptoms covered by ICD coding statistics, the average information required for each preliminary diagnosis (disease) was calculated as the threshold value. Suppose that the preliminary diagnosis obeys a random distribution p, and the interview records of a doctor obey a random distribution q. Then, cross-entropy is introduced to calculate the similarity degree of p and q. The expectation obtained according to the distribution p is *H (P)*. For the diagnosis process of doctors, the access records are discrete variables, and the p distribution is represented by the q distribution, which is called the cross-entropy.

$$H(\mathrm{p}) = \sum_i p(i) * \lg \frac{1}{p(i)} \tag{10}$$

$$H(p,q) = \sum_i p(i) * \lg \frac{1}{q(i)} \tag{11}$$

Assuming that p of a disease can be expressed as $[1, 0, 0]$ $[1, 0, 0]$, and q obtained by a doctor A's visit to the historical record is $[0.5, 0.4, 0.1]$ $[0.5, 0.4, 0.1]$, then according to the calculation method of cross-entropy of formula (11), the cross-entropy between the visit behavior of doctor in the process of diagnosis and the initial diagnosis given by doctor A can be obtained as follows:

$$\begin{aligned}
&H\left(p = [1,0,0], q = [0.5, 0.4, 0.1]\right)\\
&= -\left(1 * \lg 0.5 + 0 * \lg 0.4 + 0 * \lg 0.1\right)\\
&\approx 0.3H\left(p = [1,0,0], q = [0.5, 0.4, 0.1]\right)\\
&= -\left(1 * \lg 0.5 + 0 * \lg 0.4 + 0 * \lg 0.1\right)\\
&\approx 0.3
\end{aligned}$$

If the interview record Q of Doctor B with the same preliminary diagnosis is$[0.8, 0.1, 0.1]$ $[0.8, 0.1, 0.1]$, then, the cross-entropy between the visit and the preliminary judgment of Doctor B in the process of this diagnosis is follows:

$$\begin{aligned}
&H\left(p = [1,0,0], q = [0.8, 0.1, 0.1]\right)\\
&= -\left(1 * \lg 0.8 + 0 * \lg 0.1 + 0 * \lg 0.1\right)\\
&\approx 0.1H\left(p = [1,0,0], q = [0.8, 0.1, 0.1]\right)\\
&= -\left(1 * \lg 0.8 + 0 * \lg 0.1 + 0 * \lg 0.1\right)\\
&\approx 0.1
\end{aligned}$$

It can be seen from the calculation results that cross entropy value of Doctor B is small, that is, the operational correlation is higher. If the threshold value of this disease is known to be 0.2, then, it

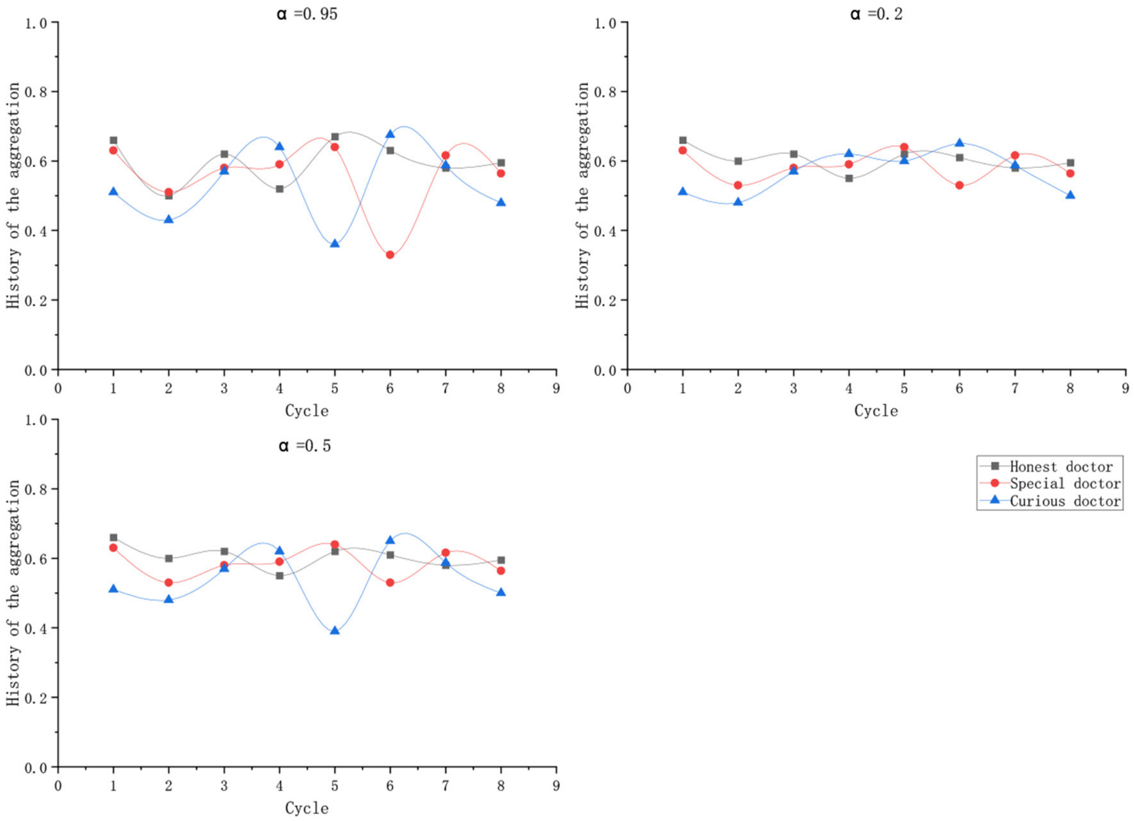

FIGURE 7 | Fluctuation of credit line.

can be concluded that Doctor B is accessing medical data safely, and Doctor A is suspected of a large privacy breach.

To calculate the accuracy of similarity, two calculation methods, namely, Jaccard coefficient and cross-entropy, were used to calculate the correlation degree of the diagnosis and treatment process. The final formula for calculating the correlation degree of the diagnosis and treatment process was as follows:

$$S=\frac{(1+\mathrm{d}_1)\,\alpha}{2H_1d_1}+\frac{(1+d_2)\,\beta}{2H_2d_2}+\frac{(1+d_3)\,\gamma}{2H_3d_3}\,(\alpha+\beta+\gamma=1) \qquad (12)$$

Because the weight cannot simply be given a definite value, it is determined by the vague advice given by experienced experts.

A review of the relevant literature and consultation with medical professionals has been discussed as follows:

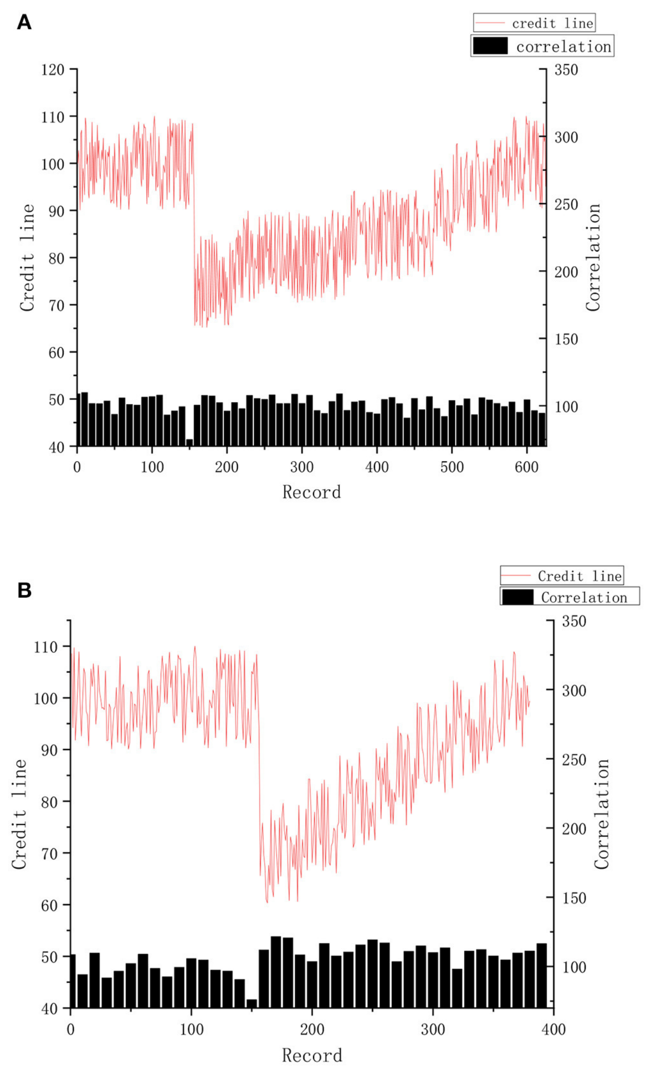

FIGURE 8 | (A,B) Change of credit limit and correlation degree.

Hypothesis A: To obtain certain medical records, a curious doctor falsifies the information of the primary diagnosis that does not match the inspection information, thereby, rationalizing the second step. However, even if qualified doctors encounter patients with special circumstances, they will not make a preliminary diagnosis with a correlation below the threshold based on the examination information of the patient. Therefore, the rules at this stage are very strong. Once the initial diagnosis is wrong, the correlation between Step 2 and Step 3 is normal, and the risk of leakage of medical record privacy is relatively high. Therefore, the weight corresponding to Step 1 needs to be relatively large. In this case, even if a curious doctor performs normal operations in Step 2 and Step 3, the credibility of the calculation will be greatly reduced.

Hypothesis B: If a qualified doctor diagnoses a patient with rare symptoms, the doctor needs to refer to more medical records to determine what disease the patient has. At this time, Step 1 is normal and the correlation of Step 2 is decreased, but according to medical records, the final judgment Step 3 should also be normal. Therefore, during the diagnosis, the weight of Step 2 can be appropriately relaxed, so that doctors can have a larger space for resource selection, and the diagnosis process of doctors in complicated cases will not be restricted.

Hypothesis C: If a curious doctor tries to imitate the behavior of an ordinary doctor in Hypothesis B, the curious doctor will naturally give a final diagnosis with low relevance to the medical record. Assuming that in the context of the medical environment, all doctors will perform their duties. A patient will not be diagnosed by only one doctor, so curious doctors will not insist on making a wrong final diagnosis to steal medical data. Therefore, in this case, the conclusion of the doctor based on a large number of irrelevant medical records will be less relevant to the initial diagnosis given by malicious intent.

Therefore, to distinguish between hypothesis B and hypothesis C, the weight of S3, namely γ, should also be large.

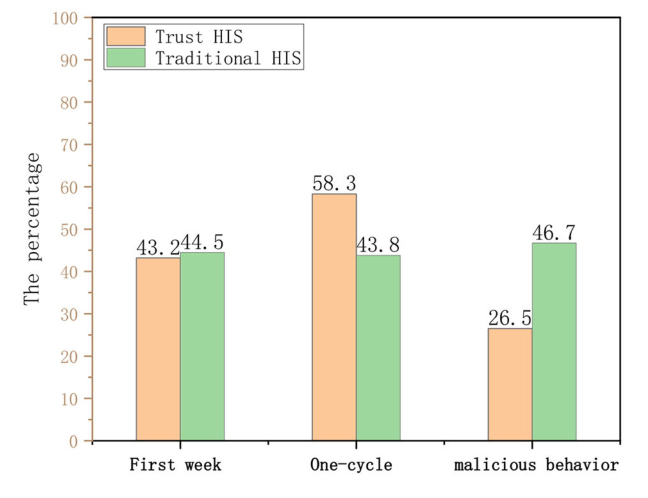

FIGURE 9 | Comparison of health information system (HIS) correlation degree and behavioral constraint ability.

According to the above hypothesis analysis, in each step, appropriate weights can provide doctors with a certain space for fault-tolerant visits or special situations requiring additional resources and can also effectively screen behaviors of curious doctors. Therefore, it is necessary to introduce appropriate weight determination technology. Xu and Zhou (42) further developed the maximum score deviation (MSD) method to obtain the weight of each index. The principle of the MSD method is that when multiple experts evaluate the evaluation factors, the higher the similarity with the evaluation of other experts, the less weight should be given. In theory, if two experts give exactly the same assessment because it does not help to draw consensus from the disagreement, the weight can be set to zero. For each expert $PF \cdot p_i$, we introduce a function $D_{ki}(x)$ to represent the scoring deviation between the evaluated step and the remaining steps:

$$D_{\mathrm{ki}}(x) = \sum_{t=1}^{N} \left| s\left(h_{ki}\right) w_k - s\left(h_{kt}\right) w_k \right| \tag{13}$$

where h_{ki} and h_{kt} are hesitation probability fuzzy numbers, $S(x)$ is a scoring function, and w_k is the weight of expert $PF \cdot p_i$ $i, t = 1, 2, ..., N$ and $k = 1, 2, ..., K$.

Thus, the total score deviation for all the steps evaluated by expert $PF \cdot p_i$ can be expressed as $D_{ki}(x)$ follows:

$$D_k(x) = \sum_{i=1}^{N} D_{ki}(x) = \sum_{i=1}^{N} \sum_{t=1}^{N} \left| s\left(h_{ki}\right) w_k - s\left(h_{kt}\right) w_k \right| \tag{14}$$

To obtain the optimal weight vector, since the general weight vector meets the normalization in cognition of people, Zhou Wei introduced constraint condition Equation (15) based on Wang (43), transformed w_k into $\overline{w_k}$ through Equation (16), and obtained the weight vector $\overline{\mathrm{w}} = (\overline{w_1}, \overline{w_2}, ..., \overline{w_k})$. In this study, a developed MSD method was adopted.

$$\sum_{k=1}^{k} (w_k)^2 = 1 \tag{15}$$

$$\overline{\mathrm{w}_k} = \frac{w_k}{\sum_{k=1}^{k} w_k} \tag{16}$$

Based on the above analysis and setting, the following objective function is constructed to obtain an optimal weight vector that can maximize the deviation value of overall scores of all doctors for each expert evaluation.

$$D(x) = \sum_{K=1}^{K} D_k(x) = \sum_{K=1}^{K} \sum_{i=1}^{N} \sum_{t=1}^{N} \left| s\left(h_{ki}\right) w_k - s\left(h_{kt}\right) w_k \right| \tag{17}$$

To solve the weight vector, the following model and Lagrange function are constructed:

$$\max \mathrm{D}(w) = \max \left\{ \sum_{K=1}^{K} \sum_{i=1}^{N} \sum_{t=1}^{N} \left| s\left(h_{ki}\right) w_k - s\left(h_{kt}\right) w_k \right| \right\} \tag{18}$$

$$s.t \begin{cases} \sum_{k=1}^{k} (w_k)^2 = 1 \\ w_k \geq 0, \quad k = 1, 2, ..., k \end{cases} \tag{19}$$

$$L(w, \eta) = \sum_{K=1}^{K} \sum_{i=1}^{N} \sum_{t=1}^{N} \left| s\left(h_{ki}\right) w_k - s\left(h_{kt}\right) \right| w_k + \frac{\eta}{2} \left(\sum_{k=1}^{k} (w_k)^2 = 1 \right) \tag{20}$$

Combined with the above formula, we can get the following:

$$\overline{w_k} = \frac{\sum_{i=1}^{N} \sum_{t=1}^{N} \left| s\left(h_{ki}\right) w_k - s\left(h_{kt}\right) w_k \right|}{\sum_{K=1}^{K} \sum_{i=1}^{N} \sum_{t=1}^{N} \left| s\left(h_{ki}\right) w_k - s\left(h_{kt}\right) w_k \right|} \tag{21}$$

According to the expert advice and MSD method, the optimal weights of each step in the similarity calculation can be obtained.

Calculation and Update of Credit Line

Aggregation of Historical Records

In the previous section, we calculated a value describing the behavior of doctors, correlation.

The historical record of each doctor is composed of calculated correlations. In a period, the doctor will generate a large number of historical records. When calculating the credit limit, the historical records are summarized according to the timeline. In the process of calculating and updating the credit limit, the time recorded in history is the time when each doctor diagnosed a certain patient. The influence of early historical records on credit lines will diminish over time. On the contrary, if the behavior of curious doctors occurs recently, the impact on credit will be even greater. As a penalty, the credit limit will remain low for a period.

Since the historical visit record is composed of similarity and time window, the value of similarity is a percentage, in the range of [0,1], so there is no need for standardization. However, the time of each historical access record needs to be mapped in the range of [0,1], that is, the data are standardized. Suppose the time window before processing is $A = (\mathrm{a}_1, \mathrm{a}_2, ..., \mathrm{a}_\mathrm{n})$, and the time window after standardization is $B = (\mathrm{b}_1, \mathrm{b}_2, ..., \mathrm{b}_\mathrm{n})$.

The mapping method is as follows:

$$B_{\mathrm{i}} = \begin{cases} \frac{a_i - (a_i)_{\min}}{(a_i)_{\max} - (a_i)_{\min}}, & a_i > 0 \\ \frac{(a_i)_{\max} - a_i}{(a_i)_{\max} - (a_i)_{\min}}, & a_i < 0 \end{cases} \tag{22}$$

To make the calculation of credit limit more objective and authentic, the earlier historical record in real life will have less impact on the current credit, that is, the longer the historical record is, its value will decay over time. Suppose the set $HT = \left\{T_{hk}\left(1 \leq k \leq q\right)\right\}\left(q = |HT|\right)$ of medical history records and the corresponding time window $B = \left\{b_k \middle| 1 \leq k \leq q\right\}$, then the time attenuation function for a task $h_k\left(1 \leq k \leq q\right)$ is as follows:

$$\phi\left(t\right) = \frac{1 - b_k/\sum_{k=1}^{q} b_k}{\sum\limits_{k=1}^{q}\left(1 - b_k/\sum_{k=1}^{q} b_k\right)} \tag{23}$$

When calculating the credit limit, the model proposed by Caverlee et al. (44) is modified. Each history record is distinguished by a time window. The structure diagram of the aggregate value calculated according to the historical record of the user in the past N cycles is shown in the **Figure 3**:

The aggregate calculation formula for history of a user $H\left(1\right) \ldots H\left(n\right)$ in the past N cycles is as follows:

$$H\left(old\right) = \frac{1}{\gamma} \times \sum_{k=1}^{N} H_K \times \alpha^{N-K} \tag{24}$$

wherein $\gamma = \sum\limits_{k=1}^{N} \alpha^{N-K}$, γ is used to limit the credit value obtained after aggregation to remain within the original credit value range; α is the adjusting parameter of the influence of historical records to the current trust evaluation. The value range of α is $0 < \alpha < 1$, the smaller the α is, the less important the historical record is.

The updated formula of the credit limit can be obtained based on the aggregate results of the above historical records:

$$H_{\text{new}} = \begin{cases} H_{\text{old}} \cdot \left[1 + \varphi\left(\Delta H\right)\right], & t > t_0 \\ H_{old} \cdot \phi\left(t\right), & t < t_0 \end{cases} \tag{25}$$

H_{old} represents the initial line of credit that is aggregated according to the historical records for the first time, H_{new} represents the value of the line of credit after constant updates, $t_0$represents the effective time of the set time window, and the time decay function. When the time interval t is less than t_0, it means that the current operation occurs within the same time window as the last one. At this time, the credit line is not updated, and the time decay function is used for processing. When t is greater than t_0, it means that within the next time window, the new aggregate value and the increment $\Delta H = H_{\text{new}} - H_{old}$ of the historical aggregate value are used to recalculate and update the value of the credit line.

DYNAMIC ACCESS CONTROL BASED ON TRUST

Overview

In this study, the concept of the credit line is introduced to improve the access control of the consultation process of doctors in the existing intelligent medical system. The doctor logs in HIS according to the identity information (the doctor logs in the device, time, place, etc.), and each user calculates the corresponding credit limit according to the system, which is used to match the reasonable permissions according to the access control strategy.

After the doctor finishes each diagnosis, the data such as the visit record from HIS will be saved in the historical record. Through trust calculation, the credit limit of the user within a period can be obtained.

The trust interval corresponds to the degree of openness of the permission. For example, the line of credit of a doctor is t (t2 < t ≤ t3). According to the access control strategy, the doctor is only allowed to visit contents with relevance of 0.6 during the diagnosis and treatment process. If the doctor visits too many irrelevant contents, the decline of the operational relevance will lead to the reduction of the credit limit of the doctor. The access request of the user is denied when the amount is insufficient. The

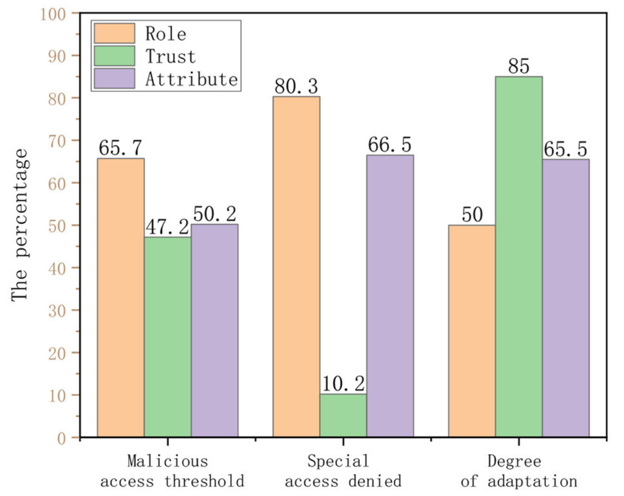

FIGURE 10 | Traditional HIS vs. trust-based access control HIS.

TABLE 6 | User evaluation table of doctors.

	Difficulty of malicious access			Risk of rejection of special access requests			Degree of system automation		
Level	I	II	III	I	II	III	I	II	III
Attribute	73	128	55	42	189	25	16	127	13
Role	156	56	44	206	34	16	116	25	15
Trust	80	84	92	10	34	212	3	64	189

credit interval of the proposed scheme and overall flow chart is shown in the **Figure 4**.

Access Control Policies

An access control policy is the key point of the access control model, which is the access rule set and condition constraint set of subject to object. In the background of the HIS system in this study, the subject is set as the doctor, and the object is the medical record. The access control flow for this article is shown in **Figure 5**.

Step 1. Read the trust value of the doctor from the library and compare the threshold $t_0(DT_i \epsilon DT, t_0 < t \leq t_4)$. The value range of T is shown in **Table 1**.

```
(a) if(DT_i.t<t_0)return false;
```

If credit limit of the doctor is below the threshold value t_0, the decision to deny access request is returned and recorded.

```
(b) if(DT_i.t≥t_0)
```

When credit line of the doctor is higher than the threshold value t_0, proceed to Step 2.

Step 2. Match the trust interval according to credit limit of the doctor:

```
(c) if (t_0 <DT_i.t≤t_1) trust = 1;
    else if (t_1 <DT_i.t≤t_2) trust = 2;
    else if (t_2 <DT_i.t≤t_3) trust = 3;
    else trust = 4;
```

If the trust value of the doctor belongs to (t_0, t_1), then 1 is returned, indicating that access rights belong to level 1.

If the trust value of the doctor is (t_1, t_2), then return 2, indicating that the access is level 2.

If the trust value of the doctor is (t_2, t_3), then return 3, which means that the access is level 3.

If the trust value of the doctor belongs to (t_3, t_4), then 4 is returned, representing that the access authority belongs to level 4.

Step 3. Match the corresponding relevance requirements according to the credit interval.

```
Switch(trust)
{
case 1 : pre(S)=0.9;
case 2 : pre(S)=0.6;
case 3 : pre(S)=0.4;
case 4 : pre(S)=0.2;
}
```

pre (S) specifies the minimum value of the access relevancy. If it is lower than this value, it will be reflected in the historical record, which will greatly affect the next round of credit evaluation.

EXPERIMENTAL ANALYSIS

Data Sources

Relying on the project of the National Natural Science Foundation of China, this study completed relevant research experiments according to the medical data set provided by a third-class hospital of Kunming, the cooperative unit of the project. The data set contains rich text data and image data, with a total of five databases, the size of which is 1,200 G, including 1,360 data tables and a total of 21,39,373 records. In this experiment, part of medical data was extracted to simulate visits of doctors in the process of diagnosis and treatment.

Experimental Settings

The purpose of the experiment is to verify whether the access control model based on HIS proposed in this study can calculate the line of credit through the historical behavior records of doctors, and well control the access rights of doctors through the value of the line of credit. The data of HIS account access records of three doctors in a department provided by the cooperative hospital were selected for calculation, including one doctor who simulated the behavior of a curious doctor and one honest doctor who simulated a special visit situation as the experimental group.

Weights

Ten medical experts were asked to directly give the weights of the relevant calculations. The weights calculated by the MSD method according to Equation (21) are shown in the **Table 2**. To verify whether the weight calculated according to the weight calculation method, MSD, is better than the weight directly given by the expert, randomly select the weights of two groups of experts and the weights calculated by the MSD method for comparison experiments.

The three doctors are honest doctors, non-malicious doctors with special circumstances (hereinafter referred to as special doctors), and curious doctors. In HIS, each doctor completed 15 diagnoses, among which the curious doctor completed three malicious behaviors, and the special doctor completed two special case diagnoses.

In addition, weights were set according to the weights directly given by Expert 3 and Expert 10 as well as the MSD calculation results, and the scatterplot drawn could intuitively see the calculation results of the correlation degree as shown in the **Figure 6**.

Maximum score deviation weights can distinguish between malicious behavior, special behavior, and normal behavior.

According to the obtained images, the analysis in the following **Table 3** can be obtained. The correlation calculated by the weight given by an expert alone cannot make an accurate judgment on the behavior of doctors, especially in the discrimination between curious doctor and special doctor.

Aggregation

According to Equation (25), with a period of 1 month, the aggregate value of historical records is used to calculate the changes in the credit lines of the three types of doctors in eight periods, as shown in the following **Table 4**:

According to the calculation, the average value of the credit line in eight periods is obtained as **Table 5**.

Three historical record influencing parameters α were given: 0.95, 0.5, and 0.2, and the credit limit of three kinds of doctors was calculated based on the aggregation of historical records in eight cycles. In the table, Δ represents the maximum fluctuation range of the line of credit under the corresponding value of α. Column $\bar{\Delta}$ records the mean fluctuation range of the line of credit.

As shown in the **Figure 7**, an appropriate α can keep the credit limit of doctors who maintain normal behavior during the diagnosis process in a relatively stable state, but they are sensitive to the malicious behavior of curious doctors.

Access Control Experiment

The period N of the historical record for the calculation of the credit limit was 1 month. Assuming that each doctor arranges 3 days a week to diagnose patients, the average daily medical record is about 50. According to the results of the experiment, when malicious visit of the doctor occurred, the credit line completely returned and stabilized at the original level, which required about 650 records, which took nearly a month. This situation is shown in **Figure 8A**.

If doctors intend to increase their average interview relevancy after malicious visits, as shown in the experimental results in the **Figure 8B**, it requires about 250 records, nearly half a month, to completely stabilize the original level of the credit line.

The experiment proves that when malicious access occurs, the value of the credit limit will be immediately affected. As punishment for privacy risk, the credit limit will be kept at a low value for a long period to warn users of their bad behavior and achieve the effect of access control at the same time.

Contrast Experiment

The hospitals that our project cooperates with are currently using traditional HIS without access control. Hundred doctors from the hospital were randomly selected for a black-box test. The doctors were divided into two groups, and the traditional HIS and the HIS of the trusted access control model proposed in this study were used for a 1 month comparison test. In the case that the doctor does not know the contents of the experiment, the historical records of the two groups of doctors are analyzed.

It can be seen from the **Figure 9** that there is no significant difference in the historical visit records (correlation) of the doctors using the two HISs within 1 week of the experiment. Throughout the experimental cycle, the relevance of doctors using traditional HIS has not changed significantly, while the trust HIS model has been significantly improved, indicating that the proposed credit line can regulate user behavior to a certain extent.

Then, we conducted a questionnaire survey of some doctors in the hospital. The purpose is to compare the credit line model proposed in this study with the role-based access control model (hereinafter referred to as role) and ABAC model (hereinafter referred to as attribute). The feedback from all 256 users is shown in the **Table 6**.

According to the table data and **Figure 10**, the following chart shows that the trust-based HIS access control model proposed in this study has a good performance in terms of flexibility of access control, preventing malicious access behavior from occurring, and the degree of system automation.

CONCLUSION

Aiming at HIS in the context of medical big data, this study proposes a dynamic access control model for doctors in the process of diagnosis and treatment. First, according to the diagnosis and treatment process of the doctor, the behavior model of the doctor is designed, and three hypotheses of privacy leakage are proposed. Then, according to the operation correlation of the doctor, time index, and other factors, the behavior of the doctor in the diagnosis and treatment process is described, and the purpose is to calculate the rationality of the diagnosis process of the doctor through mathematical methods. Finally, by calculating the credit limit, the access control strategy using the credit limit interval dynamically restricts the access ability of the doctor in the diagnosis and treatment process. Experiments prove that the model designed in this study can accurately identify bad doctors and inhibit their visits by trust value, and the ability to prevent patient privacy leakage is better than traditional HIS.

DATA AVAILABILITY STATEMENT

The raw data supporting the conclusions of this article will be made available by the authors, without undue reservation.

AUTHOR CONTRIBUTIONS

RJ proposed the idea for this paper. RJ, WW, and YY designed the study. WW wrote the paper. WW and FM performed the experimental analysis. All authors reviewed and edited the manuscript and read and approved the manuscript.

FUNDING

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

REFERENCES

1. Andreu-Perez J, Poon CC, Merrifield RD, Wong ST, Yang G-Z. Big data for health. *IEEE J Biomed Health Inform.* (2015) 19:1193–208. doi: 10.1109/JBHI.2015.2450362
2. Shi T, Ma J, Cao H, Meng L, Zhang C. Research progress of medical big data privacy protection technology. *China Med Equip*. (2019) 34:163–6. doi: 10.3969/j.issn.1674-1633.2019.05.042
3. Priyanka K, Kulennavar N. A survey on big data analytics in health care. *Int J Comp Sci Inform Technol.* (2014) 5:5865–8. doi: 10.1109/ICSSIT46314.2019.8987882
4. Dolley S. Big data's role in precision public health. *Front Public Health.* (2018) 6:68. doi: 10.3389/fpubh.2018.00068
5. Price WN, Cohen IG. Privacy in the age of medical big data. *Nat Med.* (2019) 25:37–43. doi: 10.1038/s41591-018-0272-7

6. Wang Q. Ethics predicament and protection path of medical privacy in the era of big data. *Chin Med Ethics*. (2016) 29:685–9. doi: 10.12026/j.issn.1001-8565.2016.04.43
7. Liu J. Hospital Information System (HIS) applications in the hospital[J]. *Med Inf (Surg Sect)*. (2010) 5:966–7. doi: 10.3969/j.issn.1006-1959.2010.04.214
8. Guo Z, Luo Y, Cai Z, Zheng T. Overview of privacy protection technology of big data in healthcare. *Comp Sci Explor*. (2021) 15:389–402. doi: 10.3778/j.issn.1673-9418.2009071
9. Lu X, Gu C. Analysis on causes and protective strategy of user privacy disclosure in the big data environment. *Modern Intellig*. (2016) 36:66–70. doi: 10.3969/j.issn.1008-0821.2016.11.012
10. Steinbrook R. Personally controlled online health data—the next big thing in medical care? *N Engl J Med.* (2008) 358:1653–6. doi: 10.1056/NEJMp0801736
11. Ma Z, Zhang L. Role of HIS in the modernization efforts of hospitals[J]. *Chin J Hosp Manage*. (2006) 22:350–1. doi: 10.3760/j.issn:1000-6672.2006.05.027
12. Dong J. Current status and cause analysis of hospital information system in my country[J]. *Chin J Hosp Manage*. (2003) 19:228–30. doi: 10.3760/j.issn:1000-6672.2003.04.014
13. Xue W. The research development of electronic medical records in China. *Chin Hosp Manage*. (2005) 25:17–9. doi: 10.3969/j.issn.1001-5329.2005.02.006
14. Ren L, Wang J. Lessons from the establishment and application of hospital information systems. *Chin J Hosp Manage.* (2002) 21–3. doi: 10.3760/j.issn:1000-6672.2002.05.007
15. Sandhu RS, Samarati P. Access-control-principles and practice. *IEEE Commun Mag.* (1994) 32:40–8. doi: 10.1109/35.312842
16. Hao L, Min Z, Deng G, Zhen H. Research on big data access control. Chinese *J Comp*. (2017) 40:72–91. doi: 10.11897/SP.J.1016.2017.00072
17. Mohammed I, Dilts DM. Design for dynamic user-role-based security. *Comp Secur*. (1994) 13:661–71. doi: 10.1016/0167-4048(94)90048-5
18. Thomas RK, Sandhu RS. Conceptual foundations for a model of task-based authorizations. In: *Proceedings The Computer Security Foundations Workshop VII*. Franconia, NH: IEEE (1994). p. 66–79.
19. Shen H, Hong F. Overview of access control model research. *Comp Appl Res.* (2005) 9–11. doi: 10.3969/j.issn.1001-3695.2005.06.003
20. Sandhu RS. Role-based access control. *Adv Comput*. (1998) 466:237–86. doi: 10.1016/S0065-2458(08)60206-5
21. Goyal V, Pandey O, Sahai A, Waters B. Attribute-based encryption for fine grained access control of encrypted data. In: *Proceedings of the 13th ACM Conference on Computer and Communications Security*. Alexandria, VA (2006). p. 89–98.
22. Wang X, Wang L, Li Y, Gai K. Privacy-aware efficient fine-grained data access control in Internet of medical things based fog computing. *IEEE Access.* (2018) 6:47657–65. doi: 10.1109/ACCESS.2018.2856896
23. Xu P, Huang K. The Status, Problems and Countermeasures of the Big Data of Health Care in China. *China Dig Med.* (2017) 12:24–6. doi: 10.3969/j.issn.1673-7571.2017.05.008
24. Xue T, Fu Q, Wang C, Wang X. Research on blockchain-based medical data sharing model. *Acta Automat Sin.* (2017) 43:1555–62. doi: 10.16383/j.aas.2017.c160661
25. Narayanan HAJ, Güneş MH. Ensuring access control in cloud provisioned healthcare systems. In: *Consumer Communications and Networking Conference*. Las Vegas, NV (2011). p. 247–51.
26. Wang M, Wang J, Guo L, Harn L. Inverted XML access control model based on ontology semantic dependency. *Comp Mater Continua.* (2018) 55:465–82. doi: 10.3970/cmc.2018.02568
27. Zhu Y, Huang D, Hu C-J, Wang X. From RBAC to ABAC: constructing flexible data access control for cloud storage services. *IEEE Transac Serv Comput.* (2014) 8:601–16. doi: 10.1109/TSC.2014.2363474
28. Liu Y, Zhang W, Wang X. Access control scheme based on multi-attribute fuzzy trust evaluation in cloud manufacturing environment. *Comp Integr Manuf Syst.* (2018) 24:321–30. doi: 10.13196/j.cims.2018.02.005
29. Gao P. *Research and Design of Dynamic Access Control Model Based on Trust and Role*. Tianjin: Tianjin University (2014).
30. Zhang P, Zhou L. Trust-based dynamic multi-level access control model. *Comp Modern*. (2019) 116–247. doi: 10.3969/j.issn.1006-2475.2019.07.020
31. Khan MFF, Sakamura K. Fine-grained access control to medical records in digital healthcare enterprises. *In: 2015 International Symposium on Networks*. Computers and Communications (ISNCC). Yasmine Hammamet: IEEE (2015). p. 1–6.
32. Zhang Y, Fu Y, Yang M, Luo J. Access control scheme for medical data based on PBAC and IBE. *J Commun*. (2015) 36:200–11. doi: 10.11959/j.issn.1000-436x.2015329
33. Yang Y, Zheng X, Guo W, Liu X, Chang V. Privacy-preserving smart IoT-based healthcare big data storage and self-adaptive access control system. *Inform Sci.* (2019) 479:567–92. doi: 10.1016/j.ins.2018.02.005
34. Shi M, Jiang R, Hu X, Shang J. A privacy protection method for health care big data management based on risk access control. *Health Care Manage Sci.* (2020) 23:427–42. doi: 10.1007/s10729-019-09490-4
35. Aggelidis VP, Chatzoglou PD. Hospital information systems. *J Biomed Inform*. (2012) 45:566–79. doi: 10.1016/j.jbi.2012.02.009
36. Zhang X, Fu Y, Chu P. Application of Jackard similarity coefficient in recommender system. *Comp Technol Dev*. (2015) 25:158–226. doi: 10.3969/j.issn.1673-629X.2015.04.036
37. Hamers L. Similarity measures in scientometric research: the Jaccard index versus Salton's cosine formula. *Inform Proc Manage.* (1989) 25:315–8. doi: 10.1016/0306-4573(89)90048-4
38. Niwattanakul S, Singthongchai J, Naenudorn E, Wanapu S. Using of Jaccard coefficient for keywords similarity. In: *Proceedings of the International Multiconference of Engineers and Computer Scientists*. Hong Kong (2013). p. 380–4.
39. Jamin A, Humeau-Heurtier A. (Multiscale) cross-entropy methods: a review. *Entropy*. (2020) 22:15. doi: 10.3390/e22060644
40. Dong X, Qian M, Jiang R. Packet classification based on the decision tree with information entropy. *J Supercomp*. (2020) 76:4117–31. doi: 10.1007/s11227-017-2227-z
41. De Boer PT, Kroese DP, Mannor S, Rubinstein RY. A tutorial on the cross-entropy method. *Ann Operat Res.* (2005) 134:19–67. doi: 10.1007/s10479-005-5724-z
42. Xu Z, Zhou W. Consensus building with a group of decision makers under the hesitant probabilistic fuzzy environment. *Fuzzy Optimiz Decis Mak*. (2017) 16:481–503. doi: 10.1007/s10700-016-9257-5
43. Wang YM. Using the method of maximizing deviations to make decision for multi-indicies. *Syst Eng Electron*. (1998) 20:24–6.
44. Caverlee J, Liu L, Webb S. The SocialTrust framework for trusted social information management: architecture and algorithms. *Inform Sci.* (2010) 180:95–112. doi: 10.1016/j.ins.2009.06.027

Conflict of Interest: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

Copyright © 2021 Jiang, Wu, Yu and Ma. This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY). The use, distribution or reproduction in other forums is permitted, provided the original author(s) and the copyright owner(s) are credited and that the original publication in this journal is cited, in accordance with accepted academic practice. No use, distribution or reproduction is permitted which does not comply with these terms.