Frontiers in Computing and Intelligent Systems
ISSN: 2832-6024 | Vol. 2, No. 3, 2022

Risk-based Access Control Model for Hospital Information Systems

Xue Chen

Yunnan University of Finance and Economics, School of Information, Kunming 650001, China

Abstract: With the advancement of healthcare reform in various countries, hospital information systems (HIS) and electronic medical records are developing rapidly and providing a source of power for the development of the healthcare industry. Due to the electronification of medical record information and excessive access rights of medical information systems, there is a risk of internal leakage of medical information. Therefore, based on medical information system, this paper proposes a risk-based access control model, which gets the risk value of doctors by quantifying their access behavior and divides the access interval according to the risk value for access behavior control. According to the simulation experiments, it can be seen that the model proposed in this paper is more suitable for medical scenarios than the traditional access control model.

Keywords: Access Control; Risk; Hospital Information System; Access Permissions.

1. Introduction

With the acceleration of Informa ionization in society, whether or not a hospital has a fully functional HIS has become an important indicator of its comprehensive strength. A complete HIS includes systems for outpatient management, inpatient information, drugs, electronic medical records, and medical insurance reimbursement. The coordination and cooperation among the systems improves the operation among hospitals, improves the patient's access environment, and at the same time provides data-based support for hospital management and clinical medicine. Currently, HIS mainly adopts a role-based access control model, using user-role and role-permission approaches for authorization management. The HIS with this access control model is prone to the problem of over-authorization by doctors. Doctors in the same department have the same access rights, and cannot be controlled at a fine-grained level according to their own access behavior. Therefore, this paper adds a risk quantification module on the basis of HIS to quantify the risk value caused by the doctor's access operation behavior, determine the user's access rights according to the doctor's risk value, and realize the fine-grained access of the doctor.

The rest of this paper is organized as follows. Part 2 introduces the current status of access control research at home and abroad, and analyzes the research progress and shortcomings of access control models. Part 3 introduces the risk quantification module in detail. Part 4 introduces the access control module. Part 5 conducts simulation experiments and summarizes this paper.

2. Related Work

With the development of medical information technology, more and more hospitals are using hospital information systems to carry out medical services. Currently, the issue of privacy breach of personal data has become the core concern of big data in health care. Soceanu et al proposed a new privacy protection approach for healthcare big data to address clinical data privacy and security issues by using an advanced encryption scheme, ARCANA, and an attribute-based access control authorization framework for partial visibility of authorized portions to achieve layered privacy protection of eHealth data. Hossain et al studied electronic healthcare data sharing to provide a secure model for cloud data, which can exchange information between healthcare providers and healthcare professionals, retrieve a patient's complete previous medical history without violating privacy, and reduce the probability of involuntary disclosure of personal information affecting the patient's life. To accommodate the dynamic nature and real-time authorization in big data scenarios, researchers have introduced risk into access control, enabling access control adaptivity. Wang et al assembled healthcare practical considerations to propose a practical access control approach to protect patient privacy in health information systems, allowing this model allows i.e., physicians to make access decisions while still being able to detect and control excessive access to patient medical data by quantifying the risks associated with physician data access activities. RajaniKanth Aluvalu et al proposed a dynamic attribute-based risk-aware model that combines the risk calculation and the attributes used for access control will be combined with a common access control model, which is highly dynamic. Zakaria et al roposed an IoT security risk management model for security practices in healthcare environments, which includes healthcare IoT risk management, hospital accountability metrics, and implementation phases, for the risk of IoT compromise in healthcare environments.

In response to the problem of internal leakage of medical big data as well as HIS, scholars believe that access control techniques are quite effective in solving this problem, so many scholars have expanded their research on various access control models, from the traditional access control model to the risk-based access control model that is still widely used today and the newly emerging risk-based access control and trust-based access control models. There is an increase in scholarly research on access control models, but there is less research on risk-based access control in HIS. With the development of healthcare system, risk-based access control strategy is suitable for healthcare industry with complex data to protect the privacy and security of medical data and reduce the possibility of information leakage.

3. Risk quantification

In this paper, we quantify the risk value of physician access based on the access behavior of physicians. In this paper, the risk value quantification is divided into access operation behavior, access time and access frequency for risk value quantification.

(1) Access operation behavior

There are six main operation behaviors for physicians to access cases: view, copy, download, add, modify, and delete. Different operation behaviors have different risks. The risk of only viewing is smaller than the risk of copying and downloading, and the risk of copying and downloading is smaller than the risk of adding, modifying and deleting. The risk level of viewing is set to a, the risk level of copying and downloading is set to b, and the risk level of adding, modifying and deleting is set to c. The doctor's access operation behavior over a period of time is formulated as follows

$$AP = \frac{a * Num_V + b * (Num_C + Num_D) + c * (Num_A + Num_R + Num_{De})}{Num_V + Num_C + Num_D + Num_A + Num_R + Num_{De}} \quad (1)$$

Among them, the risk levels a, b and c are set according to the actual situation, the sum of the three levels is 1, and a < b < c. NumV, NumC, NumD, NumA, NumR and NumDe denote the total number of six access operation behaviors, respectively.

(2) Access time

In the case of consultation visits, physicians usually visit cases in the case pool during on-call hours to treat the target patients. The doctor's visit time is divided into on-call and off-call hours. Usually, physicians conduct consultation visits during on-call hours. The formula for doctor's visit time during a period of time is as follows：

$$AT = \frac{Num_{AD}}{Num_{ND} + Num_{AD}} \quad (2)$$

Where NumND and NumAD denote the total number of on-duty and off-duty time visits, respectively. As the number of visits during off-duty hours increases, the higher the physician's risk value under the visit time attribute

(3) Access Frequency

When user u requests an electronic medical record in the HIS system, this paper decides based on the frequency of user u's access within the HIS for a period of time and the user's access failure rate in the service domain. The mathematical expression for the frequency of user accesses over time within the HIS is:

$$Fn_j(t) = \frac{num_t}{num_{all}} \quad (1)$$

Where 〖num〗_t denotes the number of accesses to HIS by user u in time period t, and 〖num〗_all denotes the total number of accesses to HIS by user u. 〖Fn〗_j (t)denotes the access frequency of user u in HIS in a period of time.

Based on the quantification of the three risk indicators above, and depending on the weight of each risk indicator, the risk value due to physician visit behavior is therefore.

$$Risk = \omega_1 * AP + \omega_2 AT + \omega_3 * Fn_j(t) \quad (2)$$

Where, $Risk$ is the risk value due to physician visit behavior, $\omega_1 + \omega_2 + \omega_3 = 1$ and $\omega_1 \neq \omega_2 \neq \omega_3$.

4. Access control model

The risk value of each doctor within each department can be calculated through the risk quantification module in Chapter 3. By using the K-Means algorithm for the risk value of doctors within each department, the doctors are divided into two categories and the risk value of doctors is divided into two types of risk intervals based on the clustering of doctors in the two categories, as follows.

(1) Set two initial clustering centers according to the number of doctors classified.

(2) Calculate the distance from each other point to the two clustering centers according to Equation 5, and choose the nearest one of the clustering centers as the labeled category for the unknown points.

(3) Recalculate the new centroids of each cluster after the labeled cluster centers.

(4) If the calculated new centroids are the same as the original centroids, the process ends, otherwise the second step is repeated.

$$d = \sqrt{(x_n - x_1)^2 + (y_n - y_1)^2} \quad (3)$$

Risk intervals are obtained based on the clustering results, and access is granted or denied according to the different risk intervals.

$$AccessRight = \begin{cases} Grent, & \text{Risk interval 1} \\ Deny, & \text{Risk interval 2} \end{cases} \quad (6)$$

5. Simulation experiments and summary

Table 1. Performance metrics with different ratios of over-access doctors

Proportion of over-visiting physicians	X	accuracy rate		recall rate		F1 score	
		This Model	Huizhen's Model	This Model	Huizhen's Model	This Model	Huizhen's Model
5%	15	0.71	0.65	0.27	0.22	0.50	0.46
	30	0.75	0.71	0.51	0.49	0.67	0.63
	35	0.82	0.74	0.8	0.77	0.81	0.79
	60	0.65	0.63	1.00	1.00	0.83	0.83
	75	0.53	0.53	1.00	1.00	0.77	0.77
10%	15	0.81	0.71	0.15	0.13	0.48	0.41
	30	0.84	0.79	0.34	0.24	0.59	0.51
	35	0.87	0.80	0.47	0.39	0.64	0.60
	60	0.90	0.81	0.87	0.61	0.79	0.84
	75	1.00	0.87	0.91	0.82	0.94	0.91
15%	15	0.91	0.89	0.15	0.11	0.55	0.51
	30	0.94	0.84	0.38	0.24	0.60	0.60
	35	0.96	0.89	0.49	0.39	0.61	0.60
	60	1.00	0.90	0.60	0.51	0.80	0.71
	75	1.00	0.93	0.77	0.66	0.89	0.80

In this paper, we will conduct a comparison experiment with the model proposed by Huizhen [10], in which 50

physicians' historical visit information are selected for the comparison test, and the experiment tests the superiority of the model method by three indicators: accuracy rate, recall rate and F1 score. Where, the accuracy rate indicates the proportion of over-visiting physicians among the top X physicians with the highest risk; the recall rate indicates the proportion of curious physicians among the top X physicians with the highest risk to all curious physicians; and F1 indicates the geometric mean of the accuracy rate and recall rate. The experiment sets different proportions of over-visiting doctors for 50 doctors and sets the number of visit requests to 10, and calculates the accuracy rate, recall rate and F1 score to verify the effectiveness of the model proposed in this paper.

As can be seen from Table 1, the performance of the experiment improves as the proportion of over-visiting physicians increases. As can be seen from the table, the values of the three metrics proposed in this paper basically show an increasing trend, which indicates that the performance of the model proposed in this paper gradually improves as the proportion of over-visiting physicians to all physicians rises. At the same time, the performance indexes of the model proposed in this paper have some improvement over the Huizhen model under different proportions of over-visiting doctors.

References

[1] AKHUSEYINOGLU N B, JOSHI J. A Risk-Aware Access Control Framework for Cyber-Physical Systems; proceedings of the 2017 IEEE 3rd International Conference on Collaboration and Internet Computing (CIC), F 15-17 Oct. 2017, 2017 [C].

[2] HOU M W, LAN X, XING L, et al. Study on the Application of Privacy Protection Technology in the Publication of Health Care Big Data [J]. Chin Digital Med, 2020, 15(02): 92-4.

[3] XIAO L, LI D, SUN Y, et al. Protection of personal privacy in the health and medical big data environment [J]. Chine Med Record, 2019, 20(12): 48-50.

[4] SOCEANU A, VASYLENKO M, EGNER A, et al. Managing the Privacy and Security of eHealth Data; proceedings of the 2015 20th International Conference on Control Systems and Computer Science, F 27-29 May 2015, 2015 [C].

[5] HOSSAIN A, FERDOUS S M S, ISLAM S, et al. Rapid Cloud Data Processing with Healthcare Information Protection; proceedings of the IEEE World Congress on Services (SERVICES), Anchorage, AK, F Jun 27-Jul 02, 2014 [C]. 2014.

[6] WANG Q, JIN H. Quantified risk-adaptive access control for patient privacy protection in health information systems; proceedings of the Proceedings of the 6th International Symposium on Information, Computer and Communications Security, ASIACCS 2011, F, 2011 [C]. Association for Computing Machinery.

[7] ALUVALU R, MUDDANA L. A dynamic attribute-based risk aware access control model (DA-RAAC) for cloud computing; proceedings of the 7th IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), Agni Coll Technol, Chennai, INDIA, F Dec 15-17, 2016 [C]. 2016.

[8] ZAKARIA H, ABU BAKAR N A, HASSAN N H, et al. IoT Security Risk Management Model for Secured Practice in Healthcare Environment [J]. Procedia Comput Sci, 2019, 161: 1241-8.

[9] WU X, ZHANG Y T, WANG A M, et al. MNSSp3: Medical big data privacy protection platform based on Internet of things [J]. Neural Comput Appl, 2020: 15.

[10] HUI Z, LI H, ZHANG M, et al. Risk-adaptive access control model for big data in healthcare [J]. J Comm, 2015, 36(12): 190-9.