Hindawi
Wireless Communications and Mobile Computing
Volume 2021, Article ID 5549109, 9 pages
https://doi.org/10.1155/2021/5549109

Research Article

A Model Study on Collaborative Learning and Exploration of RBAC Roles

Jiyong Yang,[1,2] Xiajiong Shen,[1,2] Wan Chen,[1,2] Qiang Ge,[1,2] Lei Zhang,[1,2,3] and HaoLin Chen[1,2]

[1]*Henan Key Laboratory of Big Data Analysis and Processing, Henan University, 475000 Kaifeng, China*
[2]*School of Computer and Information Engineering, Henan University, 475000 Kaifeng, China*
[3]*Institute of Data and Knowledge Engineering Henan University, 475000 Kaifeng, China*

Correspondence should be addressed to Lei Zhang; zhanglei@henu.edu.cn

Received 28 February 2021; Accepted 2 June 2021; Published 25 June 2021

Academic Editor: Lihua Yin

Role-based access control (RBAC) can effectively guarantee the security of user system data. With its good flexibility and security, RBAC occupies a mainstream position in the field of access control. However, the complexity and time-consuming of the role establishment process seriously hinder the development and application of the RBAC model. The introduction of the assistant interactive question answering algorithm based on attribute exploration (semiautomatic heuristic way to build an RBAC system) greatly reduces the complexity of building a role system. However, there are some defects in the auxiliary interactive Q&A algorithm based on attribute exploration. The algorithm is not only unable to support multiperson collaborative work but also difficult to find qualified Q&A experts in practical work. Aiming at the above problems, this paper proposes a model collaborative learning and exploration of RBAC roles under the framework of attribute exploration. In this model, after interactive Q&A with experts in different permissions systems by using attribute exploration, the obtained results are merged and calculated to get the correct role system. This model not only avoids the time-consuming process of role requirement analysis but also provides a feasible scheme for collaborative role discovery in multidepartment permissions.

1. Introduction

With the development of the information system, information sharing among people becomes more and more convenient and fast. However, the "explosive" growth of the information system brings people convenient and quick access to information, and it also brings the problem of information security. It is not only the sharing of information between people that needs to be protected but also the information between industrial systems. For example, when computing matrix in the research field of Kalman filtering, multiple computing contents need to be encrypted [1, 2].

To prevent the intrusion of illegal users or leakage caused by the careless operation of legal users, many solutions have been proposed [3, 4]. For example, Lihua proposes a new privacy protection scheme, which plays a good role in protecting privacy [5]. Access control allows users to access system resources only according to their permissions setting and may not exceed their permissions. To ensure flexibility and security, role-based access control (RBAC) [6] has been widely studied and applied due to its good applicability and occupies a mainstream position in the access control model [7]. The RBAC model introduces roles between users and permissions; connects users and permissions with roles and grants and revokes access permissions to users by assigning and canceling roles to users; and realizes the logical separation of users and access permissions [8]. Flexibility in permission management and its high correlation with an enterprise's organizational structure greatly facilitate permission management [9].

However, the increasing complexity of the information system leads to the increasing complexity of the RBAC model system construction [10]. In the design and use of a traditional RBAC system, the relationship between "users and roles" and

"roles and permissions" is dependent on the acquisition of system requirement information and the personal experience of administrators. With the increasing complexity and diversification of the information system, the number of users, resources, and permissions in access control is increasing, and the business process and related domain knowledge of information systems are becoming complex. As a result, designing and managing an RBAC system that meets the functional and security needs of users solely relying on human beings is challenging [11]. With the development and prosperity of machine learning has given us more ways and methods to solve problems, machine learning is applied in various fields [12]. Many scholars have also applied machine learning to information security, Sun proposes an ESS-based algorithm of balancing the QoS and privacy risk, which reaches a stable state of maintaining long-term service by multiple iterations [13], and Yin uses a recursive neural network for intrusion detection [14]. In addition, machine learning is also applied to various fields, such as hyperspectral image processing and classification [15, 16]. With the prosperity and development of information system, information security combined with many research fields has been widely discussed and studied [17, 18].

Among them, zhang Lei [19] proposed an auxiliary interactive question answering algorithm based on attribute exploration and used the attribute exploration algorithm to interact with experts to get the required roles and the partial order relationship between roles in the RBAC system. The reason why the attribute exploration algorithm [20] can obtain the roles and the partial order relationship between roles is that the attribute exploration algorithm is an important tool in the formal concept analysis [21]. Formal concept analysis is considered as a favorable tool for data analysis and knowledge description and has been widely used in data analysis [22], knowledge discovery [23], rule extraction [24], concept cognitive learning [25], and other fields. Among them, the important data structure-concept lattice [26] can well represent the partial order structure among data. Each lattice node on the concept lattice is composed of a group of intent and extent which have a natural correspondence with roles and permissions in role engineering. The role system mined by the concept lattice theory can not only reflect the hierarchical relationship between the roles but also ensure the correctness of the roles mined [27].

Although the auxiliary interactive question answering algorithm based on attribute exploration can accomplish the role design of RBAC with heuristic assistance, the traditional attribute algorithm relies on the complete system permissions knowledge. In practice, it is difficult to find people who have a good knowledge of all permissions, especially when the permissions are involved in multiple departments. For example, it is difficult to find an expert who knows all the permissions information well when constructing the role of the administration system in conjunction with the faculty system. This defect severely limits the development and application of the RBAC model.

In this paper, it is found that the Duquenne–Guigues and the set of roles obtained by the auxiliary interactive question answering algorithm based on attribute exploration have a close relationship with the whole system, but also have a close relationship with the local subsystem. Therefore, we can find an interactive domain expert in each one and merge the roles and Duquenne–Guigues of each system after the interaction of multiple systems is completed, to obtain the set of the Duquenne–Guigues and roles of the entire system.

Therefore, this paper proposes a model collaborative learning and exploration of RBAC roles (*RCLE*). Under the framework of interactive Q&A of property exploration, a method is designed to support the role discovery of the same group of users under different permission systems. This model not only avoids the time-consuming process of role demand analysis and questionnaire survey in the process of role construction but also avoids the defects of the auxiliary interactive question and answer algorithm of attribute exploration in the construction of role system across departments.

2. Basic Definition

The relevant definitions used in this article are as follows [23, 25, 26]:

Definition 1. An access security context $K=(U, M, I)$ is composed of two sets U, M, and I (the relationship between U and M). The element of U is called user (object), and the element of M is called permission (attribute). $(u, m) \in I$ or uIm means that user u has permission m. We use $(u, m) \notin I$, which means that user u does not have permission m.

Definition 2. Set $K=(U, M, I)$ that is an access security context, if $A \subseteq U, B \subseteq M$, then write

$$f(A) = \{m \in M | \forall u \in A \in \mathrm{A}, (u, m) \in I\}, \tag{1}$$

$$g(B) = \{u \in U | \forall \forall m \in B, (u, m) \in I\}. \tag{2}$$

If A and B satisfy that $f(A) = B$ and $g(B) = A$, then we call the binary group (A, B) a concept. A is the extent of the concept (A, B), and B is the intent of the concept (A, B).

The computation of Definition 2 is carried out throughout the text. Definition 2 shows how to compute concepts in a given access security context. Since more than one formal context will be involved in the following paragraphs, for the convenience of distinguishing, $f_1(A)$ and $g_1(B)$ represent the calculation of $f(A)$ and $g(B)$ on the formal context K_1.

The concept of access security context $K=(U, M, I)$ has the following basic properties ($\forall A, A_1, A_2 \subseteq U, \forall B, B_1, B_2 \subseteq M$):

Property 3. $A_1 \subseteq A_2 \Rightarrow f(A_2) \subseteq f(A_1)$; $B_1 \subseteq B_2 \Rightarrow g(B_2) \subseteq g(B_1)$; $A \subseteq g(f(A))$; $B \subseteq f(g(B))$; if $B=f(g(B))$, then B is intent on the access security context K.

Definition 4. Set (U, M, I) is an access security context, $Y \subseteq M$, and satisfies

(1) $Y \neq f(g(Y))$ $(Y \subseteq f(g(Y)))$,

(2) Each pseudointent $Y_1 \subset Y$ has $f(g(Y_1)) \subseteq Y$. Then, Y is a pseudointent.

Definition 4 provides the conditions for the establishment of pseudointent. To prove whether an attribute set is a pseudointent, we only need to verify whether it meets the two conditions of Theorem 14.

Definition 5. Set $K=(U, M, I)$ is an access security context, Y_1, $Y_2 \subseteq M$. if $g(Y_1) \subseteq g(Y_2)$, then $Y_1 \longrightarrow Y_2$ is true in K.

Definition 6. If $K=(U, M, I)$ is an access security context, then the value dependency set $\{X \longrightarrow f(g(X)) \mid X$ is the pseudointent of $K\}$ which is the Duquenne–Guigues of K.

Definition 7. Given access security context $K=(U, M, I)$, implication set $J(K)$, and implication formula $C \longrightarrow D \in J(K)$, the attribute set if and only if $T \subseteq MC \notin T$ or $D \subseteq T$, called T, is associated with $C \longrightarrow D$. If T is related to all the implication forms in $J(K)$, then T is related to $J(K)$.

According to the value dependence theory of concept lattice, the Duquenne–Guigues can produce all value dependence held in an access security context, namely, the implication relation of an attribute. It can be seen from definition 6 that the Duquenne–Guigues of access security context can be obtained as long as all pseudointents are found. The correlation judgment between attribute set and implication set in Definition 7 can be used in the calculation of pseudointent.

Definition 8. Let $K=(U, M, I)$ be an access security context, $M = \{m_1, m_2 \cdots m_n\}$, and the permission (attribute) in M satisfies the basic linear order relationship $(m_1 < m_2 < \cdot\cdot < m_n)$. For any $Y_1, Y_2 \subseteq M$ if and only if there is $m_i \in Y_2 - Y_1$ and $Y_1 \cap \{m_1, \cdots, m_{i-1}\} = Y_2 \cap \{m_1, \cdots, m_{i-1}\}$, the lexicographical order of attribute set Y_1 is less than the lexicographical order of permission (attribute)set Y_2, denoted as $Y_1 < Y_2$.

Definition 8 describes the lexicographical order relation of the property set < which is a linear order relation of 2^M. All property sets can be generated one by one according to the lexicographical order and tested one by one to see if the property set is a pseudointent or intent.

3. A Model for Collaborative Learning and Exploration of RBAC Roles

The attribute exploration algorithm interacts with domain experts by asking questions, traverses the attribute set in lexicographical order, and tests whether the set is pseudointent or intent. The use is the attribute set of the pseudointent to produce the implication, so as to construct the Duquenne–Guigues of the access security context and obtain the relevant context knowledge. Lexicographical order < is a linear order on the power set of all permission (attribute), which guarantees the completeness of the attribute exploration algorithm. In other words, the set of roles obtained by the traditional role discovery algorithm based on attribute exploration is complete. However, due to the lack of cooperation mechanism, traditional role discovery algorithms based on attribute exploration cannot build a role system across departments.

The key to the above problem is how to discover the set of roles and the implication relationship between permissions under multiple permission systems (Duquenne–Guigues). In this paper, we found that after the attribute exploration among different departments, we further analyzed and summarized the roles and Duquenne–Guigues under different permissions systems, so as to obtain the role construction of the crossdepartment permission system.

3.1. Basic Theorem. To facilitate the elaboration, we first make the following definition.

Definition 9. Given an access security context $K_1 = (U_1, M_1, I_1)$ and $K_2 = (U_2, M_2, I_2)$, $\forall g \in U_1 \cap U_2$, and $\forall b \in M_1 \cap M_2$ that meet $gI_1b \Leftrightarrow gI_2b$ then called K_1 is consistent with K_2.

Definition 10. A model for collaborative learning and exploration of RBAC roles RCLE $= (K_1, K_2, J(K_1), C(K_1), J(K_2), C(K_2))$, $K_1 = (U_1, M_1, I_1)$, $K_2 = (U_2, M_2, I_2)$, $U_1 = U_2 = \{g_1, g_2, g_3, g_4 \cdots\}$, and $M_1 = (a_1, b_1, c_1, d_1 \cdots)$, $M_2 = (a_2, b_2, c_2, d_2 \cdots)I$, represents the relationship between U_i and M. M and I are consistent in K_1 and K_2, $J(K_1)$, $J(K_2)$, $C(K_1)$, and $C(K_2)$, respectively, and represent the Duquenne–Guigues and intent of K_1 and K_2.

Based on the above definition, we have the following findings, which can be used as the theoretical basis of the RCLE model.

Theorem 11. *Given an access security context $K = (U, M, I)$, the Duquenne–Guigues $J(K)$, and implication formula $A \longrightarrow B \in J(K)$, if the attribute set is $T \subseteq M$ and if $A \subseteq T$, $B \notin T$, the attribute set T in the access security context K is neither intent nor pseudointent.*

Proof. Firstly, proof T is not intent. $A \subseteq T$, $B \notin T$, we knew from property 3 that $T \subseteq f(g(T))$, then $A \subseteq T \subseteq f(g(T))$, $f(g(A)) \subseteq f(g(T))$. Subtract A from both ends of $f(g(A)) \subseteq f(g(T))$ and get $f(g(A)) - A \subseteq f(g(T)) - A$. And because $A \longrightarrow B \in J(K)$, then $f(g(A)) - A =$ B. Because $D \notin T$, then $f(g(T)) - A \notin T$. Add A to both ends of $f(g(T)) - A \notin T$, get $f(g(T)) \notin T \cup A$. Because $A \subseteq T$, therefore, $f(g(T)) \notin T$, T, is not intent.

(2) Lastly, proof T is not pseudointent. If T satisfies the definition of the pseudointent (2), then each pseudointent $Y_1 \subset T$ must meet $f(g(Y_1)) \subseteq T$, because $A \longrightarrow B \in J(K)$. Thus, in K, A is a pseudointent. Because of $A \subseteq T$, $f(g(A)) = B \notin T$. Therefore, T does not satisfy the definition of pseudointent (2) that T is not a pseudointent in K.

Theorem 11 shows that the set of permissions (attributes) is neither intent nor pseudointent if it is not related to any implication in the Duquenne–Guigues. Because in the attribute exploration, only the set of permissions (attributes) that are intent or pseudointent are considered, and the set of permissions (attributes) that satisfy theorem 11 can be ignored and not calculated.

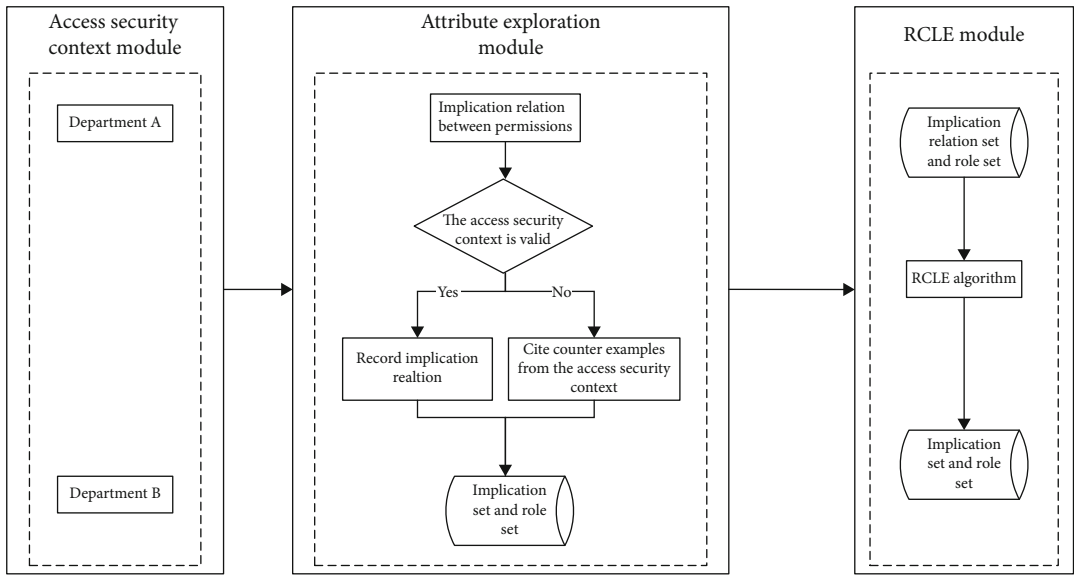

Figure 1: *RCLE* model framework.

Theorem 12. *RCLE* $= (K_1, K_2, J(K_1), C(K_1), J(K_2), C(K_2))$, $K_1 = (U_1, M_1, I_1)$, $K_2 = (U_2, M_2, I_2)$, *access security context* $K = K_1 + K_2$, *and the Duquenne–Guigues of* K *is* $J(K)$. *The permission set* D *is related to* $J(K)$, $D \longrightarrow f_1(g_1(D)) - D \in J(K_1)$. *If* $f_1(g_1(D)) \cup f_2(g_1(D)) \neq D$ *then* $D \longrightarrow f_1(g_1(D)) \cup f_2(g_1(D)) - D \in J(K)$. *If* $f_1(g_1(D)) \cup f_2(g_1(D)) = D$, *then* $f_1(g_1(D)) \cup f_2(g_1(D)) \in C(K)$.

Proof. Because D is related to $J(K)$, so by definition 7, we know that D is intent or pseudointent. $D \longrightarrow f_1(g_1(D)) - D \in J(K_1)$, then in K_1, the users that coown the permission set D are $g_1(D)$. According to definition 10, $U_1 = U_2 = U$. Because $K = K_1 + K_2$, so $f(g(D)) = f_1(g_1(D)) \cup f_2(g_1(D))$. If $f_1(g_1(D)) \cup f_2(g_1(D)) \neq D$, then D is a pseudointent; so, $D \longrightarrow f_1(g_1(D)) \cup f_2(g_1(D)) - D \in J(K)$. If $f_1(g_1(D)) \cup f_2(g_1(D)) = D$, then D is an intent, so $f_1(g_1(D)) \cup f_2(g_1(D)) \in C(K)$.

Inference 13. RCLE $= (K_1, K_2, J(K_1), C(K_1), J(K_2), C(K_2))$, $K_1 = (U_1, M_1, I_1)$, $K_2 = (U_2, M_2, I_2)$, access security context $K = K_1 + K_2$, and the Duquenne–Guigues of K are $J(K)$. The permission set D is related to $J(K)$, $D \longrightarrow f_2(g_2(D)) - D \in J(K_2)$. If $f_2(g_2(D)) \cup f_1(g_2(D)) \neq D$, then $D \longrightarrow f_2(g_2(D)) \cup f_1(g_2(D)) - D \in J(K)$. If $f_2(g_2(D)) \cup f_1(g_2(D)) = D$, then $f_2(g_2(D)) \cup f_1(g_2(D)) \in C(K)$.

Theorem 14. *RCLE* $= (K_1, K_2, J(K_1), C(K_1), J(K_2), C(K_2))$, $K_1 = (U_1, M_1, I_1)$, $K_2 = (U_2, M_2, I_2)$, *access security context* $K = K_1 + K_2$, *and the Duquenne–Guigues of* K *are* $J(K)$. *The permission set* D *is related to* $J(K)$, $D \in C(K_1)$. *If* $D \cup f_2(g_1(D)) = D$, *then* $D \cup f_2(g_1(D)) \in C(K)$. *If* $D \cup f_2(g_1(D)) \neq D$, *then* $D \longrightarrow D \cup f_2(g_1(D)) \in J(K)$.

Proof. Because D is related to $J(K)$, so by definition 7, we know that D is intent or pseudointent. $D \in C(K_1)$, and then in K_1, the users that coown the permission set D are $g_1(D)$. According to definition 10, $U_1 = U_2 = U$. Because $K = K_1 + K_2$, so $f(g(D)) = f_1(g_1(D)) \cup f_2(g_1(D))$. If $f_1(g_1(D)) \cup f_2(g_1(D)) \neq D$, then D is a pseudointent, so $D \longrightarrow D \cup f_2(g_1(D)) = D - D \in J(K)$. If $D \cup f_2(g_1(D)) = D$, then D is an intent, so $f_1(g_1(D)) \cup f_2(g_1(D)) \in C(K)$.

Inference 15. RCLE $= (K_1, K_2, J(K_1), C(K_1), J(K_2), C(K_2))$, $K_1 = (U_1, M_1, I_1)$, $K_2 = (U_2, M_2, I_2)$, access security context $K = K_1 + K_2$, and the Duquenne–Guigues of K are $J(K)$. The permission set D is related to $J(K)$, $D \in C(K_2)$. If $D \cup f_1(g_2(D)) = D$, then $D \cup f_1(g_2(D)) \in C(K)$. If $D \cup f_1(g_2(D)) \neq D$, then $D \longrightarrow D \cup f_1(g_2(D)) \in J(K)$.

Theorems 12 and 14 show that in the *RCLE* model, if a permission set is related to the Duquenne–Guigues of an access security context, then we can use the results obtained in the subdivision to carry out the union operation with the results calculated by other departments and judge whether the obtained results are intent or pseudointent.

4. RCLE Model Framework

Based on the above definitions and theorems, this section designs a model of RBAC role collaborative learning and exploration (RCLE) by referring to the framework of traditional attribute exploration algorithm and expert questions. the algorithm uses the traditional attribute exploration framework to discover the roles of different permissions system, then automatically revises the set of roles and the Duquenne–Guigues according to the obtained knowledge and the proposed theorem. In this way, we can get the required roles and the implication relationship between permissions and permissions of the system after the fusion of multiple systems. The model architecture is shown in Figure 1.

Input: two access security contexts $K_1 = (U_1, M_1, I_1)$, $K_2 = (U_2, M_2, I_2)$; Duquenne–Guigues $J(K_1)$, $J(K_2)$; intent set $C(K_1), C(K_2)$
Output: access security context K, $J(K)$, $C(K)$
BEGIN
1. $J(K)=\varnothing$, $C(K)=\varnothing$
2. $K=K_1 \cup K_2$
3. WHILE ($B \neq M$)
4. IF ($B \in C(K_1)$) THEN
5. IF ($B \cup f_1(g_2(B)) == B$) THEN
6. Add $B \cup f_1(g_2(B))$ to $C(K)$
7. ELSE
8. Add $B \longrightarrow B \cup f_1(g_2(B)) - B$ to $J(K)$
9. END IF
10. B =FindNextB($J(K), B$)
11. Continue
12. END IF
13. IF ($B \in C(K_2)$) THEN
14. IF ($B \cup f_2(g_1(B)) == B$) THEN
15. Add $B \cup f_2(g_1(B))$ to $C(K)$
16. ELSE
17. Add $B \longrightarrow B \cup f_2(g_1(B)) - B$ to $J(K)$
18. END IF
19. B=FindNextB($J(K), B$)
20. Continue
21. END IF
22. IF ($B \in J(K_1)$) THEN
23. IF ($f_1(g_1(B)) \cup f_2(g_1(B)) == B$) THEN
24. Add $f_1(g_1(B)) \cup f_2(g_1(B))$ to $C(K)$
25. ELSE
26. Add $B \longrightarrow f_1(g_1(B)) \cup f_2(g_1(B))$ to $J(K)$
27. END IF
28. B=FindNextB($J(K), B$)
29. Continue
30. END IF
31. IF ($B \in J(K_2)$) THEN
32. IF ($f_2(g_2(B)) \cup f_1(g_2(B)) == B$) THEN
33. Add $f_2(g_2(B)) \cup f_1(g_2(B))$ to $C(K)$
34. ELSE
35. Add $B \longrightarrow f_2(g_2(B)) \cup f_1(g_2(B))$ to $J(K)$
36. END IF
37. B=FindNextB($J(K), B$)
38. Continue
39. END IF
40. IF ($f(g(B)) \neq B_i$)
41. $J(K)=J(K) \cup (B \longrightarrow f(g(B)) - B)$
42. ELSE
43. $C(K)=C(K) \cup (B)$
44. END IF
45. END WHILE
46. END

Algorithm 1: RCLE algorithm description.

Using the attribute exploration algorithm, the role discovery algorithm interacts with system security managers in different departments to obtain the required set of roles (intent) and the set of implications between permissions (Duquenne–Guigues) in each department. The following is the specific process of the attribute exploration role discovery algorithm:

Input: Attribute set B, implies set $J(K)$
Output: The next attribute set NextB
BEGIN
1. B'=Find the lexicographic order of B s next
2. Flag = TRUE
3. WHILE(Flag)
4. FOR each $a_1 \longrightarrow b_1 \in J(K)$
5. IF ($a_1 \subseteq B' \&\& b_1 \notin B'$)THEN
6. B'=Find the lexicographic order of B' next
7. BREAK
8. ELSE
9. RETURN B'
10. END IF
11. END FOR
12. END

Algorithm 2: findNextB algorithm description.

At the beginning of the algorithm, the access security context is empty, the Duquenne–Guigues is empty, and the intent set is empty. Then, the set of attributes to be tested is continuously generated in lexicographic order, and an expert is asked if the implication with the attribute set as the preceding is true. If not, add a counterexample to the access security context and recalculate. If true, the attribute set is judged to be intent or pseudointent. If it is a pseudointent, then an implication form with the pseudointent added to the Duquenne–Guigues. If it is not a pseudointent, according to the value dependence of the concept lattice and the correlation theory of the attribute set, it must be intent, and then the attribute set is added to the intent set.

The set of roles and the Duquenne–Guigues obtained are substituted into the RCLE model, and the set of roles and the Duquenne–Guigues required in the system after multidepartment system fusion are calculated. At the initial stage of the algorithm, the access security context is the union of multiple access security contexts, the Duquenne–Guigues is empty, and the set of roles is empty. In line 1 of the algorithm to determine whether the algorithm has reached the end state. Inline 4-8 of the algorithm, it means that the permissions set belongs to the role set of departments 1; so, the permissions jointly owned by users in department 1 and department 2 are calculated. Line 9-13 of the algorithm indicates that the permission set belongs to the role set of department 2; so, the permissions jointly owned by users in department 2 who have B permission set are calculated in department 1. Algorithm 14-23 is the processing process of the B permission set. Line 24-28 of the algorithm is the process where B does not exist in the set of roles of department 1 and department 2, nor in their Duquenne–Guigues, where the findNextB algorithm calculates the next permission set of B' according to the correlation definition.

5. Example of the RCLE Algorithm Process

This section illustrates the running process of the RCLE model with an example. Access security context $K_1 = (U_1, M_1, I_1)$ and $U_1 = (1, 2, 3, 4)$ represents (dean of faculty, dean of

Table 1: Access security context K_1.

	f	g	h	i
1	1	1	0	0
2	0	1	0	1
3	0	0	0	0
4	0	0	1	0

Table 2: Access security context K_2.

	a	b	c	d	e
1	0	0	1	1	1
2	0	0	0	0	0
3	0	0	1	1	1
4	1	1	1	1	0

teaching, dean of research, dean of academic affairs), and $M_1 = (f, g, h, i)$represents (student curriculum management, teacher information management, graduate employment information management, scientific research information management). The specific permission information is shown in Table 1. Access security context, $K_2 = (U_2, M_2, I_2)$, $U_2 = (1, 2, 3, 4)M_2 = (a, b, c, d, e)$ represents (student information management, student registration information management, student status management, student curriculum review, student curriculum development and modification). The specific permission information is shown in Table 2. The permissions $a < b < c < d < e < f < g < h < i$。

Get by using the attribute exploration role discovery algorithm $J(K_1) = \{e \longrightarrow cd, d \longrightarrow c, c \longrightarrow d, b \longrightarrow acd, a \longrightarrow bcd\}$, $C(K_1) = \{\varnothing, cd, cde, abcd, abcde\}$, $J(K_2) = \{i \longrightarrow g, gh \longrightarrow fi, f \longrightarrow g, fgi \longrightarrow h\}$, and $C(K_2) = \{\varnothing, h, g, gi, fg, fghi\}$and plug $J(K_1)$, $C(K_1)$, $J(K_2)$, $C(K_2)$ into the RCLE algorithm.

(1) The algorithm starts at $B=\varnothing$.

(2) Because $\varnothing \in C(K_1)$, calculate $\varnothing \cup f_2(g_1(\varnothing)) = \varnothing = B$, add $\varnothing$ to the set $C(K)$, calculate the next property set of B to be i, and make $B=i$.

(3) Because $i \in J(K_1)$, calculate $f_1(g_1(i)) \cup f_2(g_1(i)) - i = g \neq \varnothing$, add $i \longrightarrow g$ to the set J(K), calculate the next property set of B to be h, and make $B=h$.

(4) Because h does not exist in $J(K_1)$, $C(K_1)$, $J(K_2)$, and $C(K_2)$,. calculate $f(g(h)) - h = abcd \neq \varnothing$, add $h \longrightarrow abcd$ to the set $J(K)$, calculate the next property set of B to be g, and make $B=g$.

(5) Because g does not exist in$J(K_1)$, $C(K_1)$, $J(K_2)$, $C(K_2)$. calculate $f(g(g)) - g=\varnothing$, add g to the set $C(K)$, calculate the next property set of B to be gi, and make $B=gi$.

(6) Because gi does not exist in $J(K_1)$, $C(K_1)$, $J(K_2)$, $C(K_2)$, calculate $f(g(gi)) - gi=\varnothing$, add gi to the set $C(K)$, calculate the next property set of B is f, and make $B=f$.

(7) Because $f \in J(K_1)$, calculate $f_1(g_1(f)) \cup f_2(g_1(f)) - f = cdeg \neq \varnothing$, add $f \longrightarrow cdeg$ to the set $J(K)$, calculate the next property set of B which is e, and make $B=e$.

(8) Because $e \in J(K_1)$, calculate $f_1(g_1(e)) \cup f_2(g_1(e)) - e = cdg \neq \varnothing$, add $e \longrightarrow cdg$ to the set $J(K)$, calculate the next property set of B is d, and make $B=d$.

(9) Because $d \in J(K_2)$, calculate $f_2(g_2(d)) \cup f_1(g_2(d)) - d=c \neq \varnothing$, add $d \longrightarrow c$ to the set $J(K)$, calculate the next property set of B is c, and make $B=c$.

(10) Because $c \in J(K_2)$, calculate $f_2(g_2(c)) \cup f_1(g_2(c)) - c=d \neq \varnothing$, add $c \longrightarrow d$ to the set J(K), calculate the next property set of B is cd, and make $B=cd$.

(11) Because cd does not exist in $J(K_1)$, $C(K_1)$, $J(K_2)$,and $C(K_2)$ calculate $f(g(cd)) - cd=\varnothing$, add cd to the set $C(K)$, calculate the next property set of B is cdg, and make $B=cdg$.

(12) ……

(13) This article will not repeat the process because of the limited space.

At the end of the algorithm, $C(K) = \{\varnothing, g, gi, cd, cdeg, cdefg, abcdh, abcdefghi\}$, $J(K) = \{i \longrightarrow g, h \longrightarrow abcd, f \longrightarrow cdeg, e \longrightarrow cdg, d \longrightarrow c, c \longrightarrow d, cdg \longrightarrow e, cdegi \longrightarrow abfh, b \longrightarrow acdh, a \longrightarrow bcdh, abcdegh \longrightarrow fi\}$.

It can be seen from the above algorithm example process that the RCLE model utilizes the traditional attribute exploration role discovery algorithm to interact with the system managers of multiple departments, so as to obtain the set of roles and the implication relation between permissions under the combination of multiple departments.

6. Experiment and Analysis

6.1. Experimental Design. In order to verify the performance of the model proposed in this paper, the random function simulation in the JAVA language MATH library is used to generate two sets of access security context as test data. The experimental design is divided into two aspects. The first aspect is to observe the change in the number of the implication relation (Duquenne–Guigues) by changing the experimental conditions. The second aspect is to change the experimental conditions to observe the changes in the number of roles (intent).

In the experiment, the algorithm traverses the access security context to answer the questions instead of the experts. The algorithm takes the randomly generated access security context as the objective access security context and traverses the entire access security context when judging whether the implication relation is true. If all users in the access security context meet the implication relation of this implication, the implication is considered to be true. Otherwise, it is considered that this implication relation is not valid, and a user is taken from the access security context and provided to the

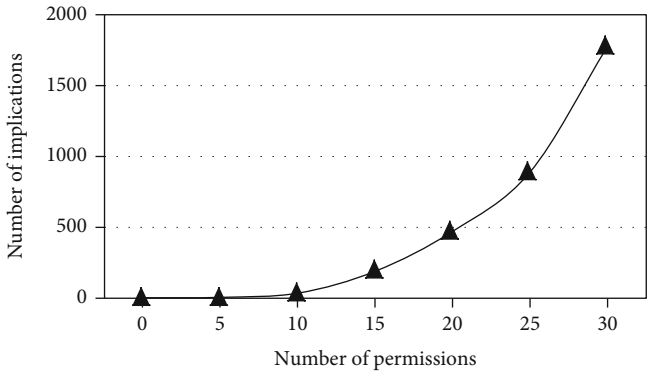

Figure 2: Number of implications (number of users: 30).

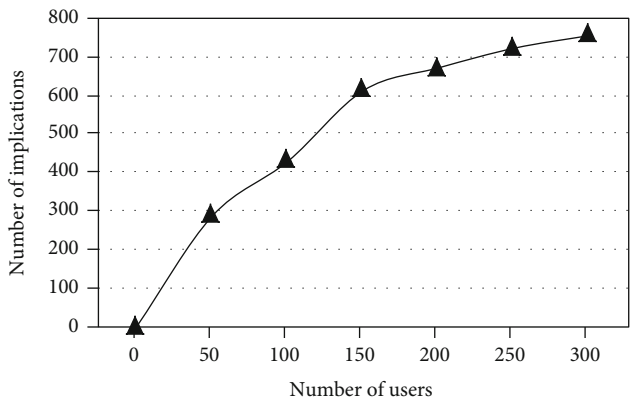

Figure 3: Number of implications (number of permissions: 15).

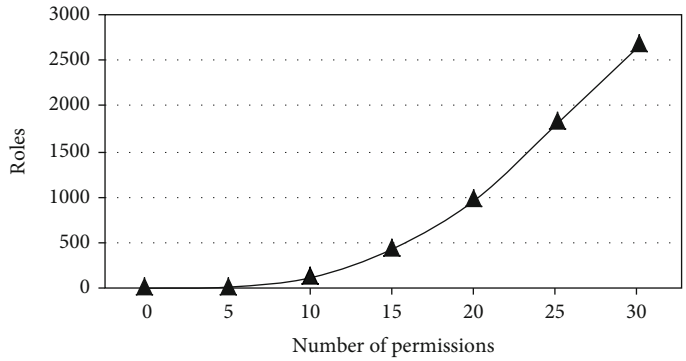

Figure 4: Number of roles (number of users: 30).

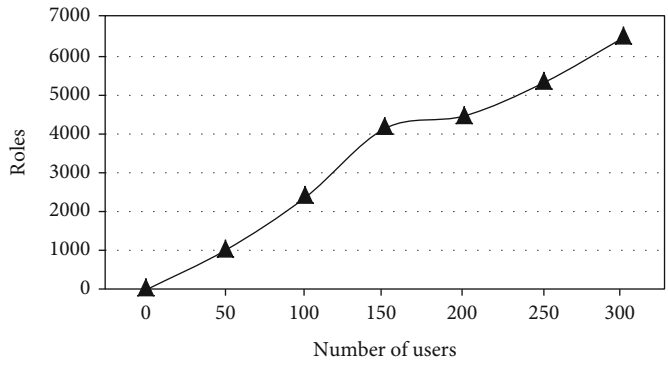

Figure 5: Number of roles (number of permissions: 15).

algorithm as a counterexample. The test platform hardware is 3.4GHZ CPU, and the 16GB memory operating system is Windows X10.

The first group of experiments sets the access security context with the same number of users (objects) and the number of permissions (attributes) from 0 to 30 at an interval of 5 to test. The purpose of the test is to fix the number of users to change the number of permissions and observe the change in the number of implications. The test results are shown in Figure 2.

The second group sets the number of access security context with the same number of permissions (attributes), and the number of users (objects) is tested from 0 to 300 at intervals of 50. The purpose of testing is to fix the number of permissions, change the number of users, and observe the change of the number of implications. The test results are shown in Figure 3.

The third group of experiments sets access security context with the same number of users (objects) and the number of permissions (attributes) from 0 to 30 at an interval of 5 to test. The purpose of the test is to fix the number of users, change the number of permissions, and observe the change in the number of roles. The test results are shown in Figure 4.

The fourth group sets the number of access security context with the same number of permissions (attributes), and the number of users (objects) is tested from 0 to 300 at intervals of 50. The purpose of the test is to fix the number of permissions, change the number of users, and watch the number of roles change. The test results are shown in Figure 5.

6.2. Experimental Analysis. The first, second, third, and fourth groups of experiments show that whether the number of fixed objects, changing the number of attributes, or the number of fixed attributes, changing the number of objects, the implication relationship, and role (intent) increase with the scale expansion of the access security context.

The RCLE model proposed in this paper not only avoids the time-consuming and labor-consuming process of role requirement analysis and questionnaire survey in the process of role construction but also solves the defects of the traditional auxiliary interactive question and answer algorithm based on attribute exploration, which does not support crossdepartments.

7. Conclusion

Because of the defect that the traditional semiautomatic heuristic method for constructing the RBAC system cannot construct a role system in different permission system departments, this paper proposes a model of RBAC role cooperative learning and exploration. Based on the local access security context, three theorems are summarized from the local point of view, and the proposed theorems are proved by mathematical rigor. Finally, a model of RCLE is given according to the theorems. The model uses the traditional attribute exploration role

discovery method to construct the role system of different permission systems, and then according to the theorem proposed in this paper, calculates the role system of the multiple departments. Because the RCLE model greatly saves the time-consuming steps in the process of role to formulate and has characteristic of the interdepartmental build role, and so here we will further the development of tools for easier operation and makes the model able to get the more extensive application and development.

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that there is no conflict of interest regarding the publication of this paper.

Acknowledgments

This work was supported by the Scientific and Technological Project of Henan Province (Grant No. 202102310340), Foundation of University Young Key Teacher of Henan Province (Grant Nos. 2019GGJS040 and 2020GGJS027), and Key Scientific Research Projects of Colleges and Universities in Henan Province (Grant No. 21A110005).

References

[1] X. Zhang, F. Ding, L. Xu, and E. Yang, "Highly computationally efficient state filter based on the delta operator," *International Journal of Adaptive Control and Signal Processing*, vol. 33, no. 6, pp. 875–889, 2019.

[2] X. Zhang, F. Ding, and E. Yang, "State estimation for bilinear systems through minimizing the covariance matrix of the state estimation errors," *International Journal of Adaptive Control and Signal Processing*, vol. 33, no. 7, pp. 1157–1173, 2019.

[3] Y. Sun, M. Li, S. Su, Z. Tian, W. Shi, and M. Han, "Secure data sharing framework Via hierarchical greedy embedding in darknets," *Mobile Networks and Applications*, vol. 26, no. 2, pp. 940–948, 2021.

[4] L. Yin, B. Fang, Y. Guo, Z. Sun, and Z. Tian, "Hierarchically defining Internet of Things security: from CIA to CACA," *International Journal of Distributed Sensor Networks*, vol. 16, no. 1, 2020.

[5] L. Yin, L. I. Ran, J. Ding, L. I. Xiao, and L. I. Ang, "δ-calculus: a new approach to quantifying location privacy," *Computers, Materials & Continua*, vol. 63, no. 3, pp. 1323–1342, 2020.

[6] R. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman, "Role-based access control models," *Computer*, vol. 29, no. 2, pp. 38–47, 1996.

[7] R. Sandhu, D. Ferraiolo, and R. Kuhn, "The NIST model for role based access control: Towards a unified standard," in *Proc ofthe 5th ACM Workshop on Role Based Access Control*, pp. 47–63, New York, NY:ACM Press, 2020.

[8] H.-C. Chen, "Collaboration IoT-based RBAC with trust evaluation algorithm model for massive IoT integrated application," *Mobile Networks and Applications*, vol. 24, no. 3, pp. 839–852, 2019.

[9] D. Ferraiolo, J. Cugini, and D. R. Kuhn, "Role-based access control (RBAC): Features and motivations," in *Proceedings of 11th annual computer security application conference*, pp. 241–248, New Orleans, Louisiana, United States, 1995.

[10] E. Bertino, "RBAC models – concepts and trends," *Computers& Security*, vol. 22, no. 6, pp. 511–514, 2003.

[11] A. Colantonio, R. Di Pietro, and A. Ocello, *Role Mining in Business:Taming Role-Based Access Control Administration*, World Scientific, 2012.

[12] D. Xu, Z. Tian, R. Lai, X. Kong, Z. Tan, and W. Shi, "Deep learning based emotion analysis of microblog texts," *Information Fusion*, vol. 64, pp. 1–11, 2020.

[13] Z. Sun, L. Yin, C. Li, W. Zhang, A. Li, and Z. Tian, "The QoS and privacy trade-off of adversarial deep learning: an evolutionary game approach," *Computers & Security*, vol. 96, article 101876, 2020.

[14] C. L. Yin, Y. F. Zhu, J. L. Fei, and X. Z. He, "A deep learning approach for intrusion detection using recurrent neural networks," *IEEE Access*, vol. 5, pp. 21954–21961, 2017.

[15] D. Xu, J. Pan, X. Du, B. Wang, M. Liu, and Q. Kang, "Massive fishing website URL parallel filtering method," *IEEE Access*, vol. 6, pp. 2378–2388, 2018.

[16] W. Huang, Y. Xu, X. Hu, and Wei, "Compressive hyperspectral image reconstruction based on spatial–spectral residual dense network," *IEEE Geoscience and Remote Sensing Letters*, vol. 17, no. 5, pp. 884–888, 2020.

[17] W. Huang, Y. Huang, H. Wang, Y. Liu, and H. J. Shim, "Local binary patterns and Superpixel-based multiple kernels for hyperspectral image classification," *IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing*, vol. 13, pp. 4550–4563, 2020.

[18] Y. Pang, L. Peng, Z. Chen, B. Yang, and H. Zhang, "Imbalanced learning based on adaptive weighting and Gaussian function synthesizing with an application on Android malware detection," *Information Sciences*, vol. 484, pp. 95–112, 2019.

[19] L. Zhang, H.-l. Zhang, D.-j. Han, and X.-j. Shen, "Theory and algorithm of role minimization problem in RBAC model based on concept lattice," *Acta Electronics Sinica*, vol. 42, no. 12, pp. 2371–2378, 2014.

[20] R. W. Ganter, *Formal Concept Analysis: Mathematical Foundations*, Springer-Verlag, Berlin, 1999.

[21] B. Ganter and R. Wille, *Formal Concept Analysis: Mathematical Foundations*, Springer Science & Business Media, 2012.

[22] L. Qin, J. Li, and Y. Wang, "Knowledge discovery based on concept lattice and its application in university employment data analysis," *Journal of Shandong University (Natural Science Edition)*, vol. 50, no. 12, pp. 58–64, 2015.

[23] X. Shen, J. Yang, and L. Zhang, "Attribute exploration algorithm based on uncorrelated attribute sets," *Computer Science*, vol. 48, no. 4, pp. 54–62, 2021.

[24] L. Wei, L. Lin, J. Qi, and T. Qian, "Rules acquisition of formal decision contexts based on three-way concept lattices," *Information Sciences*, vol. 516, pp. 529–544, 2020.

[25] Y. Mi, W. Liu, Y. Shi, and J. Li, "Semi-supervised concept learning by concept-cognitive learning and concept space," *IEEE Transactions on Knowledge and Data Engineering*, p. 1, 2020.

[26] J. Li, L. Wei, and Z. Zhang, "Concept lattice theory and method and their research prospect," *Pattern Recognition and Artificial Intelligence*, vol. 33, no. 7, pp. 619–642, 2020.

[27] C. A. Kumar, "Designing role-based access control using formal concept analysis," *Security and Communication Networks*, vol. 6, no. 3, 383 pages, 2013.