International Journal of Digital Crime and Forensics
Volume 14 • Issue 2

A Model Study on Hierarchical Assisted Exploration of RBAC

Wan Chen, Henan University, China*
Daojun Han, Henan University, China
Lei Zhang, Henan University, China
Qi Xiao, Henan University, China
Qiuyue Li, Henan University, China
Hongzhen Xiang, Henan University, China

ABSTRACT

The role-based access control (RBAC) system has been widely used in data security because of its good flexibility and security, wherein RBAC dominates the field of access control. However, the process of establishing RBAC roles is complex and time-consuming, which hinders the development and application of this field. Recently, the introduction of expert interactive Q&A algorithm based on attribute exploration has greatly reduced the complexity and time consumption of the RBAC role building process. However, when attributes increase, algorithms will face challenges that the time complexity will explode exponentially with the increase of attributes. To cope with the above problems, this paper proposes a hierarchical assisted exploration model of RBAC under attribute-based exploration expert interactive Q&A algorithm framework from the view of reducing the time consumption of overall and single role engineering. This model not only avoids the time-consuming process of single role requirements, but also reduces the time-consuming process of whole role establishment from the overall architecture perspective.

KEYWORDS

Access Control, Concept Lattice, Expert Interactive Q&A System, Formal Concept Analysis, Hierarchical Exploration, Information Security, Machine Learning, Role Engineering, System Security

INTRODUCTION

With the explosive rate of global information system, an increasing portion of information sharing is becoming an information security catastrophe. (Qiu et al., 2020) summarizes the documents in the field of information security in recent years, which indicates that information security is an urgent problem to be solved in the field of the Internet of things. The increasingly serious problem of information disclosure and security attacks has a dramatic impact on personal and national security (Michel & King, 2019).

DOI: 10.4018/IJDCF.302871 *Corresponding Author

In order to prevent the destruction or disclosure of information caused by the intrusion of illegal users or the careless operation of legal users, many scholars have proposed a variety of solutions to insure the security of the information system. Access control (Sandhu & Samarati, 1994) has gradually become a fundamental tenets of information system. Access control restricts the permissions of users to access system resources, and resources that exceed user permissions are not allowed to be accessed. The existing access control methods form two main group: autonomous control (Downs et al., 1985) and mandated access control (Jiang et al., 2004). In automatic access control, users can divert permissions directly or indirectly to other users. In spite of its great versatility and unlimited redirect ability, it makes information disclosure possible. On the other hand, the mandatory access control strictly limits the user permissions in the system, but lacks flexibility. In order to ensure the flexibility under the premise of system security, role-based access control (Samarati & Vimercati, 2011; Sandhu et al., 1996) arises at the historic moment, and dominates a mainstream position in the field of access control. The RBAC model introduces the role between users and permissions and regards roles as a bridge between users and permissions, and grants and revokes user access permissions by distributing and canceling roles to users, thus bringing about the logical separation (HC, 2019) between users and access permissions.

However, the complexity of RBAC model is getting higher and higher (Bertino, 2003) with the increasing complexity of information systems. In the design and application of traditional RBAC, system analysts and administrators restrict the relationship between "users and roles" and "roles and permissions" according to their intuitive experience and system requirements. With the research of the information system, the information system is becoming more and more complex and multifarious. In the meantime, the number of access control users and permission resources is also increasing in the system, which makes the information system face some drawbacks (Alessandro & Alberto, 2012). It is often difficult to meet the functional and security needs of users only relying on manpower to design and manage a RBAC system. On the other hand, the high time complexity about conventional RBAC systems and the unavailability to obtain the hierarchical relationship (Vaidya et al., 2007) between roles have turned out to be the fatal flaws of the conventional RBAC.

As modern machine learning advances and flourishes, it provides us with new inspirations and approaches to settle the problem. Machine learning has been widely used in a variety of areas (Zhang et al., 2014; Yin et al., 2017). An approach to mathematics (Concept lattice) (Zhang et al., 2014, Yang et al., 2021) is capable of resolving issues of the role generation. An assisted interactive quizzing algorithm based on attribute exploration is put forward, and obtained the hierarchical relationship between roles in RBAC system by using the expert interactive question and answer under attribute exploration. The partial order relation of system roles can be obtained because of the attribute exploration algorithm is a vital recipe for concept lattice (Ganter & Wille, 2012). In addition, concept lattice has recently been extensively applied in statistical analytics (Jabbari & Stoffel, 2018), knowledge discovery (Shen et al., 2020, Mahani & Baba-Ali, 2019), rule extraction (Ling et al., 2020) and access control (Chandra et al., 2018; Yang et al., 2021; Obiedkov et al., 2009).

Although the expert interactive question and answer algorithm based on attribute exploration can heuristicsly complete the establishment process of RBAC with the increase of user and permission resources, the complexity of construction process of RBAC roles will explode exponentially. Therefore, a novel hierarchical assisted exploration model based on RBAC (RHAE) is proposed from the point of view of reducing the time-consuming of the whole system and local subsystems in this paper. Under the framework of expert interactive question and answer based on attribute exploration, a method is designed to reduce the time-consuming construction of a single role while the hierarchical architecture reduces the time-consuming of the whole RBAC modeling, and also obtains the partial order relationship between roles, which greatly improves the efficiency of the construction of the whole RBAC system and greatly reduces the complexity of RBAC system management.

PRELIMINARIES

This section briefly illustrates some related fundamental notions of Formal concept analysis (FCA) and Role-based access control (RBAC) used in this article as follows:

Definition 1 (Wille et al., 2012; Duquenne et al., 1986): Supposing $K = \left(U, P, R\right)$ is an access security context which is made up of two collections U and P as well as the connection R between them, abbreviated as a formal conctext, where U is the set of users, P is a permission set, and the relationship between them is $R \subseteq U \times P$. $\left(U, P\right) \in R$ or $\left(uRp\right)$ means that the user u has a permission p. We use $\left(u, p\right) \notin R$ to indicate that the user u does not possess the permission p.

Definition 2 (Wille et al., 2012): Let $K = \left(U, P, R\right)$ be an access security context, then define the following operations in the user subset $A \subseteq U$, and the permission subset $B \subseteq P$:

$$A^I = \{p \in B \left| \right| \left. \forall u \in A, \left(u, p\right) \in R\}$$
$$B^I = \{u \in A \left| \right| \left. \forall p \in B, \left(u, p\right) \in R\}$$

A^I refers to a collection of permissions possessed by all users in A, and B^I represents a collection of users shared by all permissions in B. If for any $u \in U, \left| p \in P \right.$ there is $u^I \neq \varnothing, \left| u^I \neq P, \right| p^I \neq \varnothing, p^I \neq U$, the access security context is said to be regular.

Definition 3 (Ganter & Wille, 2012): Let $K = \left(U, P, R\right)$ be an access security context, then in the user subset $A \subseteq U$, and the permission subset $B \subseteq P$, if $A, \left| B \right.$ satisfies $A^I = B, \left| B^I = A \right.$, then we call the binary-tuple $\left(A, \left| B \right.\right)$ is an access security formal concept, abbreviated as a concept. Among them, A is the extent of the concept $\left(A, \left| B \right.\right)$, and B is the intent of the concept $\left(A, \left| B \right.\right)$.

Definition 4 (Sertkaya et al ., 2004): Suppose $K = \left(U, P, R\right)$ is an access security context, and then $Y \subseteq P$ is called the pseudo-role in K and satisfies the following conditions:

1. $Y^{II} \neq Y$;
2. For every pseudo-role $Q \subsetneq Y$ there is $Q^{II} \subseteq Y$.

Definition 5 (Stumme et al., 2005): Suppose $K = \left(U, P, R\right)$ is a formal context of access security. Let $P_1, P_2 \subseteq P$, then any formula of the form $P_1 \to P_2$ is called an implication. If there exists $P_1^{\mathrm{I}} \subseteq P_2^{\mathrm{I}}$ is valid, then the implication $P_1 \to P_2$ is valid in K.

Definition 6 (Guigues et al., 1986; Lakhal & Stumme, 2005): Suppose $K = \left(U, P, R\right)$ is an access security context, and the set of implication:

$$Imp\left(K\right) = \{P \to P^{II} \setminus P \left| \right| \left. P \ is \ a \ pseudo - intent \ of \ K\}$$

is the Duquenne-Guigues Base of K.

Definition 7 (Ganter & Wille, 2012): The Duquenne-Guigues Base of K is a dependency base with non-redundant, completeness and correctness.

Definition 8 (Ganter & Wille, 2012; Stumme et al., 1996): Suppose $K=\left(U,P,R\right)$ is an access security context, the permission set $P=p_1,\cdots,p_n$, if the basic linear order given on P is $\left(p_1<p2<\cdots<p_n\right)$, then for any $B_1,B_2\subseteq P$ there exists $B_1<B_2$ iff $p_i\in B_2-B_1$ exists and:

$$B_1\cap\left\{p_1,\cdots,p_{i-1}\right\}=B_2\cap\left\{p_1,\cdots,p_{i-1}\right\}$$

Definition 9 (Zhao & Qin, 2009): Suppose $K=\left(U,P,R\right)$ is an access security context, the permission set $P=p_1,\cdots,p_n$, if the basic linear order given on P is $(p_1<p2<\cdots<p_n)$, then the lexicographical relationship $<$ of the permission set in the formal context K is the linear order relationship of 2^M. According to the lexicographical relationship, the permission set can be tested one by one whether the permission set is an intent (role) or pseudo-intent (pseudo-role) in the access security context K.

Definition 10 (Zhao & Qin, 2009): Suppose $K=\left(U,P,R\right)$ is an access security context, and the set of implication $Imp\left(K\right)$ has the implication form $C\to D\in Imp\left(K\right)$. If there exists $C\subseteq T$ and $D\subsetneq T$ for the permission set $T\subseteq M$, then T is not related to $C\to D$. If the permission set T is not related to any one of implications in $Imp\left(K\right)$, then it is said that T is not related to $Imp\left(K\right)$.

Definition 11 (Shen et al., 2020): Suppose $K=\left(U,P,R\right)$ is an access security context, and $Imp\left(K\right)$ is the Duquenne-Guigues Base of K. As for any one implication $C\to D\in Imp\left(K\right)$, if the permission set T is not related to the implication $C\to D$, then T is neither a role nor pseudo-role K.

A RBAC MODEL FOR HIERARCHICAL ASSISTED EXPLORATION

To facilitate the following elaboraion, this article sets definitions in advance as follows.

Theoretical Basis

Definition 12: Let $K=\left(U,P,R\right)$ is an access security context, permission set $B,B^+\subseteq M$, if $B<B^+$ and the interval $\left\langle B,B^+\right\rangle$ is an empty set, then it is said that B^+ is only greater than B, which is recorded as $B^+\succ B$.

Definition 13: Let $K=\left(U,P,R\right)$ is a formal context of access security and a Duquenne-Guigues Base $Imp\left(K\right)$ on K, any implication $C\to C^{II}-C\in Imp\left(K\right)$. If there is a permission set $B^+,\left|N\in M\right.$ satisfies $B^+>B$ and B^+ is not related to the Duquenne-Guigues Base $Imp\left(K\right)$, $B\precsim N$ and N is related to $Imp\left(K\right)$. Then there is neither a role nor pseudo-role in the interval $\left\langle B,\min\left(B^{II},\left|N\right.\right)\right\rangle$.

Definition 14: Suppose $K=\left(U,P,R\right)$ is an access security context, and the permission set $P=p_1,\cdots,p_n$, if the basic reverse linear order given on P is $(p_1>p2>\cdots>p_n)$, then the

lexicographic relationship $>$ of the permission set is a reverse linear order relationship of 2^M in the formal context. According to the reverse lexicographical relationship, the permission set can be tested one by one whether the permission set is a role or pseudo-role in the formal context K.

Definition 15: Let $K=\left(U,P,R\right)$ is an access security context, the permission set $P=p_1,\cdots,p_n$, if the basic reverse linear order given on P is $(p_1>(p_2>\cdots>p_n)$, according to the reverse linear order, all permission sets of K can be constructed as a prefix dictionary tree (the permission sets of the parent node is actually contained in the permission sets of the child node and the sibling nodes follows the reverse linear order).

Based on the above definitions, the following findings in this paper can be used as theoretical basis for further improving roles discovery process of RBAC.

Theorem 1: Let $K=\left(U,P,R\right)$ is an access security context, any one implication $C\to D\in Imp\left(K\right)$. If permission set $T=C\cap D$, then T is a role set.

Proof: Since $C\to D\in Imp\left(K\right)$, we know that $D=C^{II}-C$ by Definition 6, then $T=C\cap D=C\cap\left\{C^{II}-C\right\}=C^{II}$. That is, $T=C^{II}$. From Definition 6, we can see that $T^{II}=C^{IIII}=C^{II}=T$, namely T is a role set.

Theorem 1 brings to light that if permission set only composed of the antecedent and consequent of any one implication in the Duquenne-Guigues Base, then these permission sets must be roles. Because the Duquenne-Guigues Base is only obtained by the implication of the pseudo-role sets in the process of RBAC, the permission sets that satisfy Theorem 1 do not need to calculate the corresponding implications.

Theorem 2: Let $K=\left(U,P,R\right)$ is an access security context, any one implication $C\to D\in Imp\left(K\right)$. According to Definition 14, the reverse linear order of the sub-nodes of C in the dictionary prefix tree is $C_1>C_2>\cdots>C_n$. If $D\subseteq\left\langle C_n,C_1\right\rangle$, then the nodes from the largest child node C_1 to D (including the D node) is not related to $Imp\left(K\right)$, so it does not exist pseudo-role or role in the interval $\left\langle D,C_1\right\rangle$. If $D<C_n$ (the smallest node of C), then all child nodes except for $C\cup D$ of C are neither role nor pseudo-role in this layer. If $D>C_1$ (the largest node of C), then all child nodes of C are neither role nor pseudo-role in this layer.

Proof: According to the Definition 15, the sub-nodes of C can be set as $\left(C_1,C_2,\cdots,C_n\right)\subset C$ in the prefix dictionary tree. If $D\subseteq\left\langle C_n,C_1\right\rangle$, so for any permission set $T\subseteq\left\langle D,C_1\right\rangle$ contains the antecedent and does not include the consequent of the implication $C\to D\in Imp\left(K\right)$, then it can be known that permission sets T in this layer are neither a role nor pseudo-role set from Definition 11. If $D<C_n$ (the smallest node of C), then when $T=C\cup D$, T must be a role set in the light of aforementioned Theorem 1. Moreover, the other child permission nodes of C besides $T=C\cup D$ contain the antecedents C and not contain the consequent D of $C\to D\in Imp\left(K\right)$ in this layer. Then we can see that all child nodes except for $C\cup D$ of C are neither role nor pseudo-role set from definition 11 in this layer. If $D>C_1$ (the largest node of C), then permission set D must be an upper-layer node of all child nodes of C in the prefix dictionary tree. It can be seen that all child nodes of C must contain the antecedent and does

not include the consequent of the implication $C \to D \in Imp\left(K\right)$, so all child nodes of C are neither role nor pseudo-role set from definition 11 in this layer.

Theorem 2 illustrates that, if the permission sets of this layer are contained in the interval between any one known implication subsequent and the largest child node of the implication antecedent in the Duquenne-Guigues Base in the prefix dictionary tree, then there are neither a role nor pseudo-role permission set in this interval. This provides a theoretical basis for skipping the calculation of these permission sets when hierarchically judging these permission sets are roles or pseudo-roles in the inner layer of the prefix dictionary tree.

Theorem 3: Suppose $K = \left(U, P, R\right)$ is an access security context, if $D = \varnothing$ for any one implication $C \to D$, then the implication $C \to D$ must be valid in the formal context K, and the permission set C must be a role.

Proof: For any one implication $C \to D$ and $D = \varnothing$, the implication $C \to D = C \to \varnothing$. And in an access security context $K = \left(U, P, R\right)$, there is $C^I \subseteq U = \varnothing^I$, so any one implication $C \to \varnothing$ is true in K. And the implication $C \to \varnothing$ holds in the formal context K, so $\varnothing = C^{II} - C$ namely $C^{II} = C$, so the permission set C must be a role.

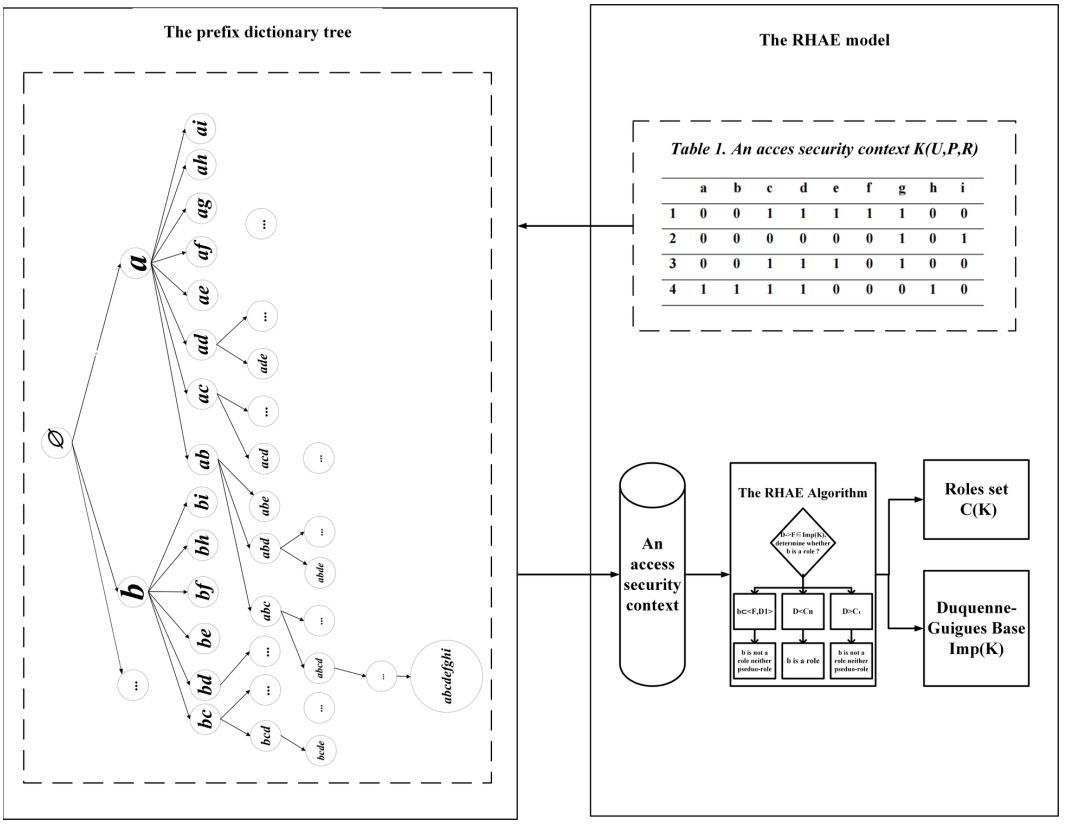
Theorem 3 promulgates that, if the consequent permission of any one implication is an empty set when judging implications in the access security context, then the implication must be valid in the given formal context, and the antecedent permission set of the implication must be a role. Because the Duquenne-Guigues is only obtained by implications of the pseudo-role permission sets in the process of RBAC, the implications that satisfy Theorem 3 do not need to be judged whether it is valid in the given access security context.

The Model and Algorithm of RHAE

Based on the relevant theories of previous RBAC literature and the basic theorems proposed in previous section. This section designs a RBAC hierarchical assistant exploration model (RHAE) under the framework of traditional attribute exploration expert interactive question and answer. The difference between this model and the traditional attribute exploration model and the traditional RBAC model in the process of role discovery of RBAC is that, RHAE constructs a prefix dictionary tree according to the cardinal order between layers and the reverse linear order inner-layer. In this way, RHAE can make use of the three theorems proposed to skip a substantial number of permission sets corresponding role and implication calculations are neither role nor pseudo-role in previous section, which greatly decreases the search space for role discovery permission sets and enhances the efficiency of the whole model. The overview of RHAE model is shown in Figure 1. Specifically, it can be seen that RHAE first obtains all sets of permissions according to the formal context in the upper right corner, then stores the sets of permissions in inter-level cardinality order and intra-level reverse linear order based on the prefix dictionary tree structure on the left, and then skips a large number of corresponding roles and implication calculations for RBAC system role generation according to the theorems presented in the previous section.

In order to obtain the role permission set (Roles) and potential relationship between user permissions and permissions (Duquenne-Guigue Base) needed by the whole RBAC system, the role discovery of RBAC system is carried out according to the corresponding RHAE model algorithm. The specific process of RHAE algorithm is shown in Algirithm 1. Suppose the scale of the access security context is $U \times M$. In the RHAE algorithm, all permission sets need to be divided into M layers, so the time complexity of the entire process layering is $O(M)$. When the algorithm calculates the first-layer permissions, it needs to traverse the formal context once for the first-layer permission

Figure 1. Overview of RHAE model



b and to calculate b^{II} once, so for the first-layer permission sets, the time complexity is $O(U \times M)$. In each of the following layers, the irrelevance of any attribute set b to the implications in Duquenne-Guigues Base is related to the scale of the Duquenne-Guigues Base, because the scale of Duquenne-Guigues Base is related to the scale of the formal context, but the relationship is not very clear. Therefore the scale of Duquenne-Guigues Base can be set as P, then the complexity of calculating a single attribute set b unrelated to Duquenne-Guigues Base in each layer is $O(M \times P)$. Similarly, for any one permission set b in each layer, the time complexity of computing b is whether composed of any one implication antecedent and subsequent in Duquenne-Guigues Base is $O(M \times P)$. Finally, for each layer of pseudo-role set implication calculation, it is still necessary to traverse the formal context once, that is, the time complexity is $O(U \times M)$. Therefore, the worst time complexity of the RHAE algorithm is $O\left(\max\left(U, M\right)P^2\right)$. U, M is the scale of user set and Duquenne-Guigue Base respectively. In addition, our RHAE also obtains the implicit relationship between the permissions of users in RBAC system.

EXPERIMENTAL EVALUATION

In order to evaluate the performance of our proposed RHAE model, this paper uses the random function in the MATH library to generate a set of test data as the access security context. The experimental design is divided into four groups. In the first group, to change the number of RBAC system users and observe the changes of system roles with user. In the second group, to change the number of RBAC

Algorithm 1. PAEUIS Algorithm Description

Input: An access security context $K=\left(U,P,R\right)$.

Output: Duquenne-Guigues Base $Imp\left(K\right)$, Roles set $C\left(K\right)$

BEGIN

1. $k=1, B\left[k\right]=\left\{\varnothing\right\}\cup P\left[k\right], Imp\left(K\right)=\varnothing, C\left(K\right)=\varnothing$
2. For all permission sets b in $B\left[k\right]$ in hierarchical do
3. If $b^{II}==b$ then
4. b is a role, $C\left(K\right)=C\left(K\right)\cup\left\{b\right\}$, and skip the implication calculation of permission set b.
5. Else
6. $Imp\left(K\right)=Imp\left(K\right)\cup\left\{b\rightarrow b^{II}-b\right\}$
7. End if
8. Wait for termination of all hierarchical processes in this layer.
9. End for
10. $Imp_{k-1}\left(K\right)=Imp\left(K\right), C_{k-1}\left(K\right)=C_{k}\left(K\right)$
11. While $k<\left|P\right|$ do
12. $k=k+1$
13. For all permission sets b in $B\left[k\right]$ in hierarchical do
14. If $b\subseteq\left\langle F,D_{1}\right\rangle$ (Theorem 2), F is the consequent of any one implication $D\rightarrow F\in Imp_{k-1}\left(K\right)$, D_{1} is the largest child node of D, then
15. b is neither a role nor pseudo-role, skip the implication calculation of permission set b.
16. Else if $D<C_{n}$ (Theorem 2), C_{n} is the smallest node of C, then
17. When $b=C\cup D$, b is a role, skip the implication calculation of other permission sets.
18. Else if $D>C_{1}$ (Theorem 2), C_{1} is the largest node of C, then
19. b is neither a role nor pseudo-role, skip the implication calculation of permission set b.
20. End if
21. If b is unrelated to $Imp_{k-1}\left(K\right)$ then
22. b is neither a role nor pseudo-role, skip the implication calculation of permission set b.
23. End if
24. If b is consisted of an antecedent and consequent (Theorem 1) of any one implication $Imp_{k-1}\left(K\right)\left[i\right]$ in $Imp_{k-1}\left(K\right)$ then
25. b is a role, $C_{k}\left(K\right)=C_{k-1}\left(K\right)\cup\left\{b\right\}$ skip the implication calculation of permission set b.
26. End if
27. If $b^{II}-b==\varnothing$ (Theorem 3) then
28. b is a role, $C_{k}\left(K\right)=C_{k-1}\left(K\right)\cup\left\{b\right\}$ skip the implication calculation of permission set b.
29. End if
30. $Imp_{k}\left(K\right)=Imp_{k-1}\left(K\right)\cup\left\{b\rightarrow b^{II}-b\right\}$
31. Wait for termination of all hierarchical processes in this layer.
32. End for
33. End while
34. $Imp\left(K\right)=Imp_{k}\left(K\right), C\left(K\right)=C_{k}\left(K\right)$
35. Return Duquenne-Guigues Base $Imp\left(K\right)$, Roles set $C\left(K\right)$.

system permissions and observe the changes of system roles with permission. The third group, to fix the number of permissions in RBAC system, we compared RHAE algorithm with traditional attribute exploration algorithm (TAE) based on RBAC, unrelated attribute exploration algorithm (AEUS) and the latest parallel attribute exploration algorithm (PAE) to observe the relationship between role generation and time-consuming. As for fourth group, we fixed the number of users in RBAC system and compared with TAE, AEUS and PAE to observe the relationship between role generation and time-consuming. The experimental test platform is 3.3GHz 's CPU and 16G memory Windows10 operating system, the test platform software is IDEA 2021.2, JDK9, and the code language is Java.

In the first experiment, RBAC system access security context users have the 20 system permissions, and the quantity of users is increased from 0 to 100 with a step size of 20. The intention is to observe the changes of the generation of system roles with the change of system users by fixing the system users' permissions. The experimental results are shown in Figure 2.

In the second set of experiments, the number of RBAC system users is 20, and the number of system permissions is evaluated incrementally from 0 to 50 with a step size of 10. The purpose is to observe the changes of the role generation of system according to the change of permissions owned by the system users by fixing the number of system users. The experimental results are shown in Figure 3.

Through the first and two groups of experiments, we find that the role generation of RBAC system increases with the increase of users or users' permissions. Interestingly, comparing figure 2 and figure 3, we find that the increment of the number of system roles generated is more dramatic than that of system users when system permissions increases, which indicates that the demand for users' permission is intenser than that for users in RBAC system.

The third group of experiments set the number of RBAC system users are 20 in the access security context, the number of permissions from 0 to 50 with a step size of 10 for incremental testing. The purpose is to change the number of permissions in the access security context and observe the changes of the role generation time of each RBAC system algorithm. The experimental results are shown in Figure 4.

The fourth group of experiments set the RBAC system users have 20 permissions in the access the security context, the number of users from 0 to 50 with a step size of 10 for incremental testing. The purpose is to change the number of users in the access security context and observe the changes of the role generation time of each RBAC system algorithm. The experimental results are shown in Figure 5.

Figure 2. The number of roles with users change

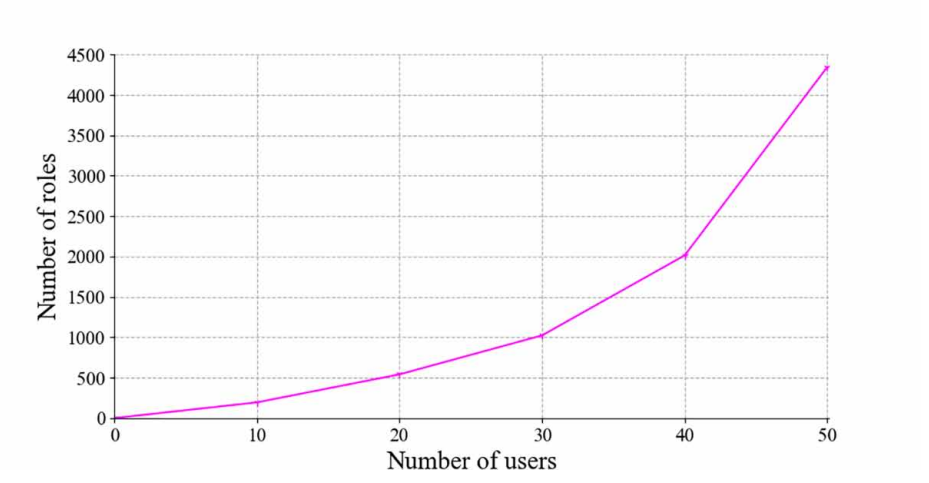


Figure 3. The number of roles with permissions change

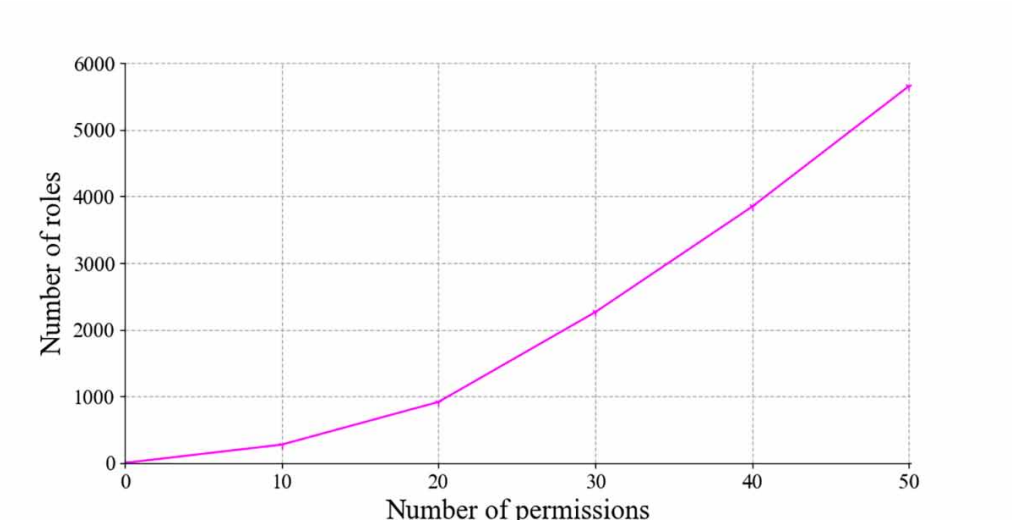
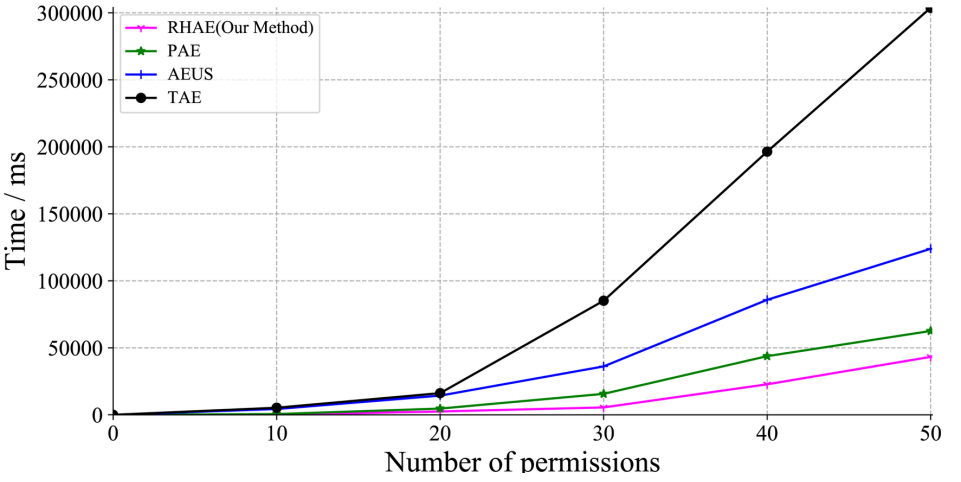
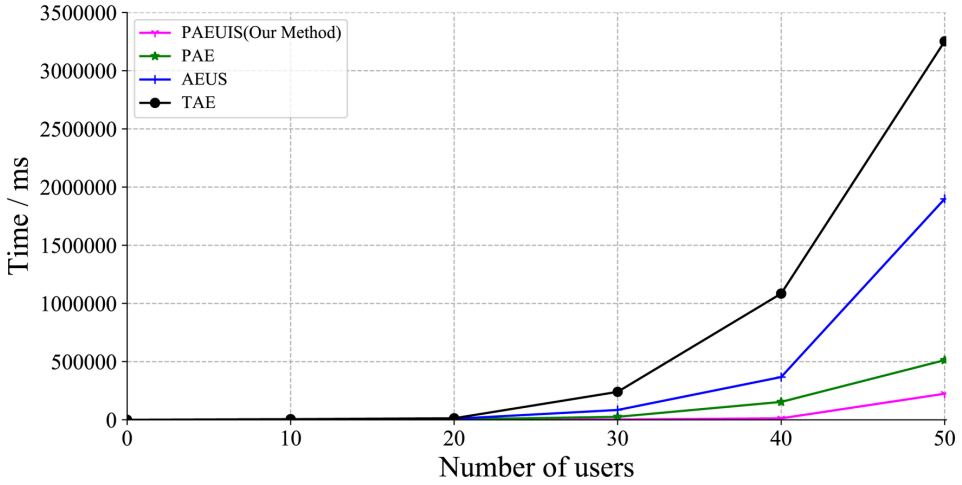


Figure 4. The consuming-time of permissions change



Through the third and fourth group of experiments, It can be seen that the RHAE algorithm improves significantly relative to other algorithms both as the number of system users with the number of permissions grows and or users grows. It is obvious that our RHAE algorithm has obvious advantages in terms of time-consuming compared with TAE, AEUS and PAE algorithms with the increase of system users (permissions), and outperforms the best in the process of role generation in RBAC system. In addition, our RHAE also obtains the implicit relationship between permissions of users in RBAC system.

Figure 5. The consuming-time of users change



CONCLUSION

Under the framework of traditional RBAC system role generation algorithm, this paper considers the problem that system role generation time will increase exponentially when system users or permissions increase sharply from the point of view of reducing the overall system time and local subsystem time. Based on previous theories of RBAC and attribute exploration, this paper puts forward the relevant definitions and theorems, and gives a RHAE model according to these theorems. According to these theorems proposed in this paper, this model greatly reduces the search space for role generation in many permission sets, and greatly improves the efficiency of role generation in RBAC system. As a next step, we intend to consider the use of the RHAE model for medical library staff role management and collaborative learning in multiple access control contexts.

ACKNOWLEDGMENT

This research was supported by the Scientific and technological project of Henan Province (Grant No. 202102310340, 212102210414); Foundation of University Young Key Teacher of Henan Province (Grant No. 2019GGJS040, 2020GGJS027); and Key scientific research projects of colleges and universities in Henan Province (Grant No. 21A110005).

FUNDING AGENCY

Open Access Funding for this article has been covered by the authors of this manuscript.

REFERENCES

Alessandro, C., & Alberto, O. (2012). *Role mining in business: taming role-based access control administration*. World Sci. doi:10.1142/9789814366151_0003

Baader, F., & Sertkaya, B. (2004). Applying formal concept analysis to description logics Concept Lattices, *Second International Conference on Formal Concept Analysis, ICFCA* (pp. 261-286). Springer.

Bertino, E. (2003). RBAC models—concepts and trends. *Computer & Security, 22*, 511–514. 10.1016/S0167-4048(03)00609-6

Chen. (2019). Collaboration IoT-based RBAC with Trust Evaluation Algorithm Model for Massive IoT Integrated Application. *Mobile Netw Appl., 24*, 839–852. 10.1007/s11036-018-1085-0

Downs, D. D., Rub, J. R., Kung, K. C., & Jordan, C. S. (1985). Issues in discretionary access control. *IEEE Symposium on Security and Privacy*, 208-208. doi:10.1109/SP.1985.10014

Ganter, B., & Wille, R. (2012). *Formal concept analysis: mathematical foundations*. Springer Science & Business Media.

Guigues, J., & Duquenne, V. (1986). *Familles minimales d'implications informatives résultant d'un tableau de données binaires*. Academic Press.

Jabbari, S., & Stoffel, K. (2018). A Methodology for Extracting Knowledge about Controlled Vocabularies from Textual Data using FCA-Based Ontology Engineering. *IEEE International Conference on Bioinformatics and Biomedicine (BIBM)*. doi:10.1109/BIBM.2018.8621239

Jiang, Y., Lin, C., Yin, H., & Tan, Z. (2004). Security analysis of mandatory access control model. *IEEE International Conference on Systems, Man and Cybernetics, 6*, 5013-5018 doi:10.1109/ICSMC.2004.1400987

Lakhal, L., & Stumme, G. (2005). Efficient mining of association rules based on formal concept analysis. In Lecture Notes in Computer Science. Springer. https://doi.org/10.1007/11528784_10.

Mahani, A., & Baba-Ali, A. (2019). New rule-based knowledge extraction approach for imbalanced datasets. *Knowledge and Information Systems, 61,* 1303-1329.

Michel, M. C. K., & King, M. (2019). Cyber infuence of human behavior: personal and national security, privacy, and fraud awareness to prevent harm. *IEEE International Symposium on Technology and Society (ISTAS)*. doi:10.1109/ISTAS48451.2019.8938009

Obiedkov, S., Kourie, D., & Eloff, J. (2009). Building access control models with attribute exploration. *Computers & Security, 28*, 2-7.

Qiu, J., Tian, Z., Du, C., Zuo, Q., Su, S., & Fang, B.J. (2020). A survey on access control in the age of internet of things. *IEEE Internet Things Journal, 7*(6), 4682-4696. 10.1109/JIOT.2020.2969326

Sabrina, P., & Vimercati, S. (2011). Access control: Policies, Models, and Mechanisms. New-York: Springer US.

Sandhu, R., Coyne, E., Feinstein, H., & Youman, C. (1996). Role Based Access Control Models. *IEEE Computer*, *29*(2), 38–47. doi:10.1109/2.485845

Sandhu, R.S., & Samarati, P. (1994). Access control: principle and practice. *IEEE Communications Magazine, 32,* 40-48. <ALIGNMENT.qj></ALIGNMENT>10.1109/35312842

Shen, X., & Yang, J., & Zhang, L. (2020). Attribute Discovery Algorithm Based on Unrelated Attribute Sets. *Computer Science*.

Shen, X., Yang, J., Zhang, L., & Yang, G. (2020). An interactive role learning and discovery model for multi-department rbac building based on attribute exploration. *Journal of Ambient Intelligence and Humanized Computing*, 1–10.

Subramanian, C. M., Kumar, C. A., & Chelliah, C. (2018). Role based access control design using three-way formal concept analysis. *International Journal of Machine Learning and Cybernetics*, *9*(11), 1807–1837. doi:10.1007/s13042-018-0840-7

Vaidya, J., Atluri, V., & Guo, Q. (2007). The role mining problem: fnding a minimal descriptive set of roles. In *Proceedings of the 12th ACM symposium on Access control models and technologies* (pp. 175–184). doi:10.1145/1266840.1266870

Wei, L., Liu, L., Qi, J., & Qian, T. (2020). Rules acquisition of formal decision contexts based on three-way concept lattices. *Information Sciences, 516*, 529-544.

Yang, J., Shen, X., Chen, W., Ge, Q., Zhang, L., & Chen, H. (2021). A Model Study on Collaborative Learning and Exploration of RBAC Roles. Wireless Communications and Mobile Computing.

Yang, J., Shen, X., Chen, W., Ge, Q., Zhang, L., & Chen, H. (2021). A Model Study on Collaborative Learning and Exploration of RBAC Roles. *Wireless Communications and Mobile Computing*, *2021*, 1–9. Advance online publication. doi:10.1155/2021/5549109

Yin, C., Zhu, Y., Fei, J., & He, X. (2017). A deep learning approach for intrusion detection using recurrent neural networks. *IEEE Access, 5*, 21954–21961.

Zhang, L., Zhang, H., Han, D., & Shen, X. (2014). Theory and algorithm of role minimization problem in RBAC model based on concept lattice. *Acta Electronics Sinica, 42*, 2371-2378.

Zhao, X., & Qin, P. (2009). On Attribute Exploration Algorithms. *Journal of Frontiers of Computer science & Technology*.

Daojun Han received Ph.D. degree in 2011. He is a professor at the School of Computer and Information Engineering, Henan University, Kaifeng, China. His major study fields include information security, knowledge discovery and spatial data process.