Enterprise Knowledge Access Control Based on Colored Petri Net

Xiaozhong Li*, Xiaoqin Liu, Ying Liu, Peng Zhao

College of Computer Science and Information Engineering, Tianjin University of Science and Technology, Tianjin 300222 China

*email: lixz@tust.edu.cn

Abstract. In the era of knowledge economy, knowledge management has been recognized as an important means to enhance the competitiveness of enterprises, and the access control of enterprise knowledge is a main mechanism of information system security. In this article, through analyzing the type of enterprise knowledge, we will build an enterprise knowledge access control model based on colored Petri net. In this model, we can use the different colors of token to distinguish the type of enterprise knowledge, so as to implement different access strategies. It makes access to the knowledge of the enterprise more efficiently and safely.

1 Introduction

Access control [1] in information system is very important, and it is a matter of system security problems. In addition, it plays a crucial role in the normal operation of information systems.

However, the traditional access control is described using access control matrix, which is mainly based on the user's identity or authorized entity. But the static access control permission does not consider the system status or the object of treatment, when information system deals with the task [2]. Therefore, establishing scientific and rational enterprise knowledge access control model is the foundation of secure access. Traditional Petri net has good mathematical property and the ability of describe asynchronous concurrent, so it will provide the help to build access control model for knowledge. However, there have shortcomings, when built more complex knowledge flow system [3]. Firstly, the same knowledge tokens led to knowledge type single. Secondly, we can't set different access strategy according to the importance of the knowledge. However, colored Petri net overcomes the drawback of the above [4].

In the end, this paper proposes the model of enterprise knowledge access control based on colored Petri nets. We will use different colors identification of different types of knowledge, so it solved the knowledge type single fault [5]. On the other hand, knowledge has category, so we can access knowledge with different strategies. This model makes access to enterprise knowledge more efficiently, safely and hierarchically.

2 Access control

2.1 The basic concept of access control

Access control: it is a measure to prevent unauthorized using resources, so as to ensure the availability of resources confidently and integrally.

Subject: any entity who can request access to the application system, including all kinds of users, the application of the interface and the illegal invaders. System must have the ability to recognize, so the key is to examine the legitimacy of the user's identity. Therefore, the system must set recognition mechanism to authenticate users identify.

User: the user can access to data independent in a computer system, and user is a person in most cases.

Authority: authority is a visit pass in the system of data resources.

Role: role is an organization or a position, which is the symbol of a kind of qualification, rights and responsibility.

2.2 access control model

The goal of access control is to prevent unauthorized access to any resources, to ensure that only legitimate subject to access object. Traditional access control contains role-based access control (RBAC) [6], task-based access control (TBAC), mandatory access control (MAC) and role-based and task-based access control (R&TBAC). The RBAC and TBAC are inflexible.   R&TBAC is the most flexible, efficient. MAC control is too strong. WebFlow access control model is based on R&TBAC, and has increased resources, tasks, and external constraint, as shown in figure 1:
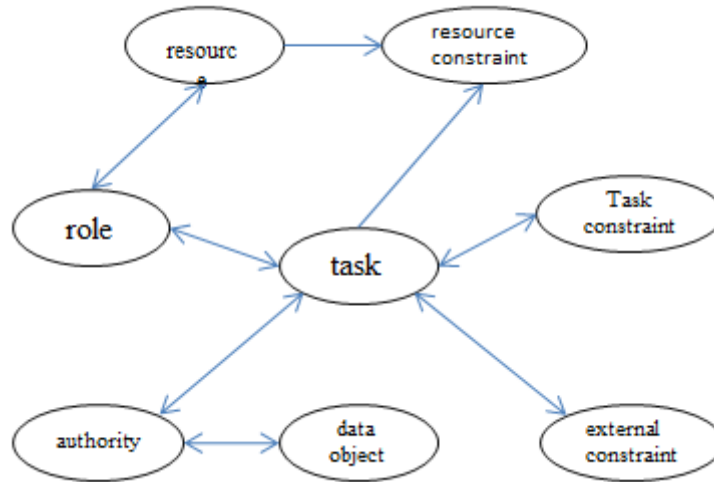

Figure 1 access control model

Resources and tasks are assigned to roles, and permissions are assigned to the task. According to different permissions, data object assigned to the task. Resource, in system operation, has a certain role to perform a task, and then obtains access permissions to the data [7]. According to the need to access the object, it will perform different tasks, thus the required permissions are also different.

3 Colored Petri net

Petri net is suitable to describe concurrent characteristic in the system [8]. It has strict formalization definition and intuitive graphical representation. Colored Petri net (Colored Petri Net, CPN) extended color based on traditional Petri net, and then become high-level Petri net. It not only inherits the traditional all advantages of Petri nets, but also enhances the logical expression ability though a color set of place, arc expression, the guard function and so on. At the same time, it also has the characteristics of flexible express, so modeling method based on CPN completely has the ability of access control model. It can adapt to complicated enterprise business processes [9].

Colored Petri net for the basic Petri net expansion mainly embodied in the token, which can use different colors represent different objects. In addition, we can define arc expression function and protecting function in colored Petri net to control colored token. The specific definition as follows:

Definition: colored Petri net can be represented as a collection, namely CPN = {S, P, T, F, C, M0, E, G}, among them:

Σ - limited set of non-empty class called the color set, and it determines the color set for network type, operation and function of annotation.

P - the finite set of place.

T -the finite set of transition.

F -the finite set of arc, $P \cap T = P \cap A = T \cap A = \emptyset$

C - color function, C: P - > Σ, each place are mapped to a set of color. That is to say, every token of the P (token) belongs to the color type C (P).

M0 –the initial state of net.

E - arc expression functions, and meet:

$\forall a \in A : [\text{Type}(E(a)) = C(p(a))_{MS} \wedge \text{Type}(\text{Var}(E(a))) \subseteq \Sigma]$

G - guard function, and meet:

$$\forall\, t \in T : [\mathrm{Type}(G(t)) = \mathrm{Bool} \wedge \mathrm{Type}(\mathrm{Var}(G(t))) \subseteq \Sigma], \mathrm{Bool} = \{\mathrm{true}, \mathrm{false}\}$$

4 the enterprise knowledge access control model based on colored Petri net

4.1 colored Petri net model

The information transmission and process are the core contents of Enterprise information system. In addition, the safe of the information also is one of the key problems of information system [10]. Access control is the main mechanism to ensure the security of information system. Enterprise knowledge types are various, if we can take different access strategies according to different types of knowledge, it will make enterprise knowledge hierarchy and more efficient access to knowledge. At this point, the colored Petri net is adopted to classify enterprise knowledge and uses different access mechanisms to the different types of knowledge, and then we establish enterprise knowledge access control model based on colored Petri net [11]. As shown in figure 1, the meaning of place and transition is shown in table 1.
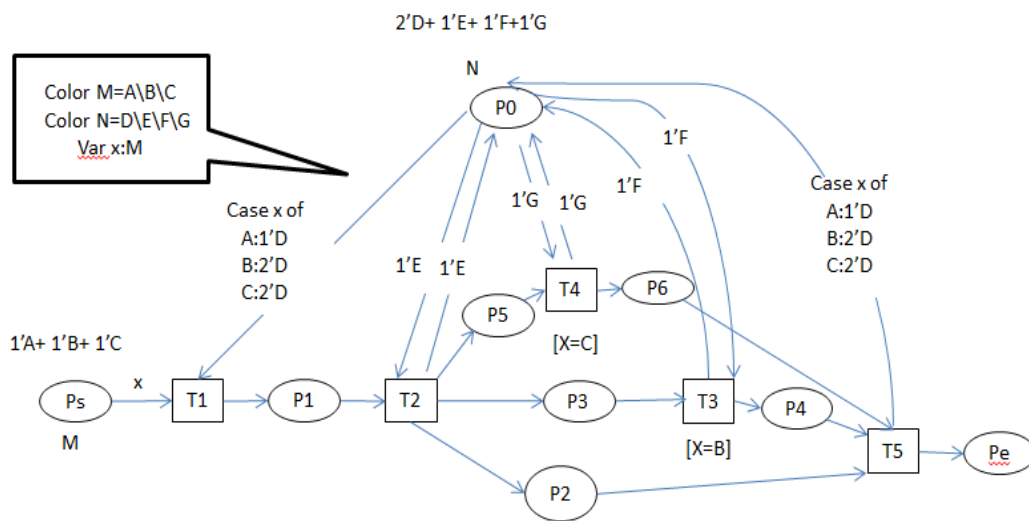

Figure 1 Enterprise knowledge access control based on colored Petri net

Table 1 the meaning of the place and transition in the model of enterprise knowledge access control based on colored Petri net

place	meaning	transition	meaning
Ps	starting place	T1	survey data information
P0	resource library	T2	department audit
P1	information	T3	leadership audit
P2	department audit completed	T4	chairman audit
P3	department audit completed	T5	information arranges
P4	leadership audit completed		
P5	department audit completed		
P6	chairman audit completed		
Pe	termination place		

4.2 model analysis

For figure 1, the process description is as follows. General enterprises tend to adopt different access strategies, when subject access object which have different importance. The enterprise knowledge can be divided into common knowledge, core knowledge and confidential knowledge [12]. The process of access to common knowledge is: survey data information→department audit→ information arranges. The process of access to core knowledge is: survey data information→ department audit→leadership audit→ information arranges. The process of access to confidential knowledge is: survey data information→department audit→chairman audit→ information arranges. Among them, the place indicates status information and transition indicates handling process.

Model defines two sets: Color M = A\B\C and Color N = D\E\F. Among them, M represents

knowledge type: A is common knowledge, B is core knowledge, C is confidential knowledge; N represents personnel: D is ordinary employees, E is department manager, F is enterprise leadership and G is chairman for the enterprise. The initial state of the model is set to M0= [3,5,0,0,0,0,0 ,0,0] ,which is 1'A + 1' B +1' C and 2' D +1'E + 1' F + 1'G, and it said that the human resource has two ordinary employees, a department manager , an enterprise leadership and an enterprise chairman; Task object have common knowledge, core knowledge and confidential knowledge each one.

In addition, the model defines the arc expression function and guard function. Arc expression function decides increase or decrease to the number of the token in system. Only when the token in the transition of the change process, enter place P have certain quantity and color of the token is greater than or equal to the number of the corresponding arc function definition, then it can make the transition. For example (P0, T1), a case of x: A: '1 D;B: '2 D;C: 2 'D, if access to common knowledge needs only an ordinary employee, but access to knowledge as the core knowledge and confidential knowledge need two staff members. Transition represents possible task or action in system. Only when the guard function return value is true, it can make the transition to be fired into the next node status. In figure 1, transition T3 and T4 have guardian function [X = B] and [X] = C. It can be performed, only when the guard function value is "True". In other words, when access to knowledge as the core knowledge, transition T3 will perform. When access to confidential knowledge, transition T4 will perform.

Based on colored Petri net access control model [13], it not only clearly describes different access mechanisms to different types of knowledge, but also describes the whole process of access control resource usage. In-depth analysis of the model, we can get diagram of model as shown in figure 2, when deal with common knowledge access control process; we can get reach diagram of model as shown in figure3, when deal with core knowledge access control process; we can get reach diagram of model as shown in figure 4, when deal with confidential knowledge access control process.
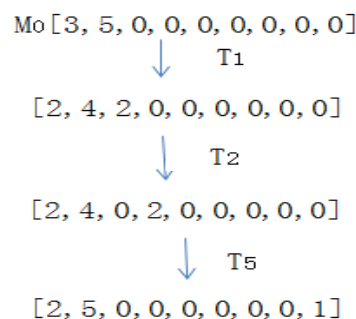
Mo[3, 5, 0, 0, 0, 0, 0, 0, 0]
↓ T1
[2, 4, 2, 0, 0, 0, 0, 0, 0]
↓ T2
[2, 4, 0, 2, 0, 0, 0, 0, 0]
↓ T5
[2, 5, 0, 0, 0, 0, 0, 0, 1]

Figure2 reach diagram of access to common knowledge

Mo[3, 5, 0, 0, 0, 0, 0, 0, 0]
↓ T1
[2, 3, 3, 0, 0, 0, 0, 0, 0]
↓ T2
[2, 3, 0, 0, 0, 0, 3, 0, 0]
↓ T4
[2, 3, 0, 0, 0, 0, 0, 3, 0]
↓ T5
[2, 5, 0, 0, 0, 0, 0, 0, 1]
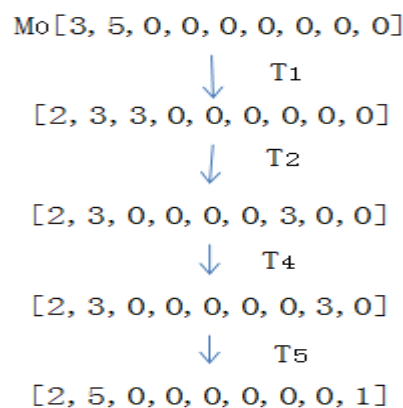
Figure3 reach diagram of access to core knowledge

```
Mo[3, 5, 0, 0, 0, 0, 0, 0, 0]
              ↓    T₁
[2, 3, 3, 0, 0, 0, 0, 0, 0]
              ↓    T₂
[2, 3, 0, 0, 3, 0, 0, 0, 0]
              ↓    T₃
[2, 3, 0, 0, 0, 3, 0, 0, 0]
              ↓    T₅
[2, 5, 0, 0, 0, 0, 0, 0, 1]
```
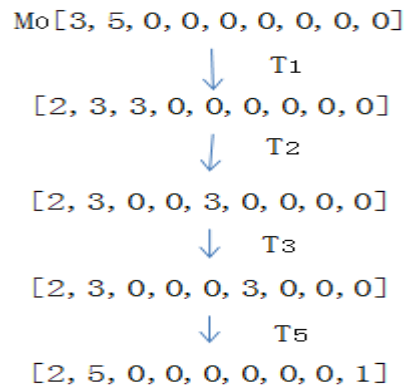
Figure 4reach diagram of access to confidential knowledge

From figure 2, figure3, figure 4,we know that every transition enables in the model. Depending on the access object, there have three great transition sequences: L1:T1→T2→T5; L2: T1→ T2→ T4→T5;L3:T1→T2→T3→T5.When access to common knowledge, token from the initial place Ps via great transition sequence L1 get to final place Pe ; When access to core knowledge, token from the initial place Ps via great transition sequence L2 get to final place Pe; When access to confidential knowledge, token from the initial place Ps via great transition sequence L3 get to final place Pe, no inaccessible place or deadlock in the model.

In this model, enterprises can make different colors of token represent different types of knowledge. Namely, it is necessary to classify enterprises knowledge, and it is beneficial to management enterprise knowledge more efficiently and we also can rapid access knowledge. Besides, according to the categories of knowledge, enterprises can set different access mechanisms. The common knowledge can make simple and quick access strategy, and the important knowledge can make strict access strategy. It not only improves the efficiency of knowledge access, but also improves the safety to the important knowledge.

5 Conclusion

Access control is an important security protection strategy of information system. In addition, it limits the main access to resources, so as to guarantee the reliability and availability of information resources system. Traditional access control usually uses the two-dimensional matrix, and it is static. In other words, it can't vary with different access strategy, when we access different objects. All the knowledge is same to knowledge system, because there is no category. That is to say, we can't set different access strategy according to the importance of the knowledge.

Based on colored Petri nets of enterprise knowledge access control model, on the one hand, it provides a reference for enterprise knowledge classification. On the other hand, it also provides an important reference value for enterprise, when they want to manage different categories of knowledge with different strategies.

Acknowledgement

References

[1] Daxin Liu, Weifang Chen. Dynamic access control based on Petri net workflow [J]. Microcomputer development, 2004, 14 (2) : 100-103.

[2] Ren Ying, Jianming Wang. Dynamic access control technology of workflow based on colored Petri net [C] / / the 22nd China academic conference proceedings database (technical report). 2005.

[3] Peterson J L. Petri net theory and the modeling of systems[M].Prentice Hall, PTR,1981.

[4] Yijie Ding, Xiaozhong Li. Based on colored Petri net knowledge flow modeling and analysis [J]. Journal of system simulation, 2011,23(7) : 287-290.

[5] Jensen K, Kristensen L M, Wells L. Colored Petri Nets and CPN Tools for modeling and validation of concurrent systems[J]. International Journal on Software Tools for Technology Transfer, 2007, 9(3-4):213-254.

[6] Meng Jian, Liming Cao, Xiaoping Wang and so on. Petri net of role-based access control model and the negotiation tree [J]. Journal of tongji university: natural science edition, 2007, 35 (6) : 815-819.

[7] Peterson J L. Petri net theory and the modeling of systems[M].Prentice Hall, PTR,1981.

[8] Jensen K. Colored Petri Nets. Basic Concepts, Analysis Methods and Practical Use[C]// Analysis Methods, Monographs in Theoretical Computer Science. Springer Publishing Company, Incorporated, 1996:493-493.

[9] Junyan Qi. The research and application of transaction workflow model based on colored Petri net [D]. Dalian university of technology, 2006.

[10] Olivier M S, Van d R R P, Gudes E. Specifying Application-level Security in Workflow Systems[C]// Proceedings of the 9th International Workshop on Database and Expert Systems Applications. IEEE Computer Society, 1998:346-346.

[11] Chen Dan. Scientific research and application of workflow system based on colored Petri [D]. Guangdong university of technology, 2014.

[12] Rodríguez-Elias O M, Martínez-GarcíaA I, Vizcaíno A, et al. A framework to analyze information systems as knowledge flow facilitators[J]. Information & Software Technology, 2008, 50(6):481–498.

[13] Dongsheng Liu. Modeling workflow processes with colored Petri nets. Computers in Industry,2002,49(2):267-281.