Contents lists available at YXpublications

International Journal of Applied Mathematics in Control Engineering

Journal homepage: http://www.ijamce.com

Research on Fine-Grained Access Control Model Combining Attributes and Trust

Jiaming Zhao[a,*], Jie Sun[b], Xiaofeng Quan[b], Hongbin Zhang[b]

[a] *Qiqihar University, Qiqihar 161000, China*

[b] *State Grid Heilongjiang Electric Power Company Qiqihar Power Supply Company, Qiqihar 161006, China*

ARTICLE INFO

Article history:
Received 28 January 2021
Accepted 2 April 2021
Available online 5 April 2021

Keywords:
Attribute Authentication
Trust Computing
Fine-Grained
Dynamic
Decoupling

ABSTRACT

Because the traditional access control technology is static and coarse-grained, the control level is highly coupled, which causes great difficulties for computer security defense. In response to the above problems, an access control model combining attributes and trust is proposed. Refine roles into organizational positions and business roles to achieve the first-level decoupling of roles and permissions. Introduce the concepts of job attributes, and business attributes to authenticate users. Establish a trust evaluation mechanism, and at the same time add job attribute values and business attribute values into the trust calculation, realizing dynamic authorization in a trusted environment. At the same time, the concept of service is added, and the trust relationship is established in the mapping relationship between business roles and services, which realizes the second-layer decoupling of roles and permissions, and at the same time, ensures the fine-grained authorization of the system. Transform the traditional static authorization model into a credible, fine-grained, and dynamic authorization model. At the same time, it realizes the dual protection of system data resources, prevents system information from being damaged by illegal operations, and can effectively curb the malicious behavior of illicit users.

1. Introduction

With the rapid development of computer technology, various significant data loss, and user information theft accidents frequently occur due to system security defense problems, and access control technologies[1-4] have emerged. The access control technology is an integral part of ensuring system information security. By restricting subject access to objects specified by access control technology, information resources are not used illegally, and the security of system resources is guaranteed. It is the most basic and most important part of computer systems—security Mechanism. In the historical process of access control technology research, autonomous access control DAC and mandatory access control MAC have appeared successively[5-6]. However, autonomous access control will cause system security problems due to its poor flexibility. Mandatory access control does not support the integrity protection of system resources, which will cause limitations. The subsequent role-based access control RBAC[7-8] Makes up for the shortcomings of DAC and MAC and gradually becomes the mainstream access control technology. However, with the development of databases, networks, and distributed computing, RBAC has been bound to permissions and roles after users are assigned roles. Dynamic adjustments and fine-grained allocation of permissions cannot be performed, resulting in rigid access control mechanisms and poor flexibility. The system's scalability is not enough, making the information system unable to prevent illegal network attacks actively, and there is a risk of substantial information leakage. Domestic and foreign scholars have researched the traditional role-based access control model[9-10]. Literature [11] introduced the concept of trust in the computing environment, granting permissions to users by roles and trust, thereby improving the security of the access process. Literature [12] proposed an RBAC model based on trust and reputation and realized A new method of calculating the direct trust value improves the security of the model and has good scalability. Still, it does not solve the problem of coupling between permissions. The trust and role-based approach proposed in [13] The dynamic access control model, which adds the entity element of service, realizes the decoupling of roles and permissions but does not consider the threat of the user's first access to the system. Literature [14] admits the decoupling between roles and permissions, But system security needs to be improved.

To better solve this problem, this paper combines attributes and trust based on the traditional access control model. It proposes a fine-grained access control (RBAC combining Attributes and Trust, AT-RBAC) model that combines attributes and trust. This model

[*] Corresponding author.
E-mail addresses: 2324254702@qq.com (J. ZHAO)

realizes the two-layer decoupling between roles and permissions by fine-graining roles into organizational positions, business roles, and service levels while ensuring the fine-grained authorization of the system; establishing an attribute authentication mechanism and trust evaluation Mechanism to make the system subject to double-layer security protection; by introducing position attributes and business attributes into the trust calculation, the system’s trust dynamic authorization is guaranteed. The system is protected from illegal damage, and the system’s security is improved.

2. A fine-grained access control model combining attributes and trust

By fine-graining roles into organizational positions, the mapping between organizational positions and business roles is established; through the mapping layer and centralized management of role assignment restrictions, the purpose of separating the user's part from the business undertaken by the position is achieved, and the job level is reduced. The impact of changes on the business layer, to achieve the first-level decoupling between role and authority; organizational position is determined by the two dimensions of the organizational department and organizational role, so organizational positions are specifically realized in organizational departments; at the same time, organizational positions It is a many-to-many relationship with business roles to mapping, which realizes multi-dimensional fine-grained division.

Establish an attribute authentication mechanism by screening job attributes and business attributes to ensure the integrity of user attributes and realize the first layer of security protection of the system. Establish a trust evaluation mechanism, introduce user attributes into trust calculation, and complete trust authorization verification — the second layer of system security protection. Through trust authorization verification, a dynamic trust relationship is established between business roles and services to ensure the security and dynamics of the authorization process. The service concept is introduced to achieve the second layer of decoupling between roles and permissions, increase the trust threshold at the service level, establish a mapping trust bond between business roles and restrictions so that the security of each subsequent step of authorization meets the system requirements. The model is established through double-layer decoupling and double-layer security protection. It solves high role-privilege coupling, inadequate security, and coarse-grained in the traditional access control model. Figure 1: Fine-grained access control model based on attributes and trust.

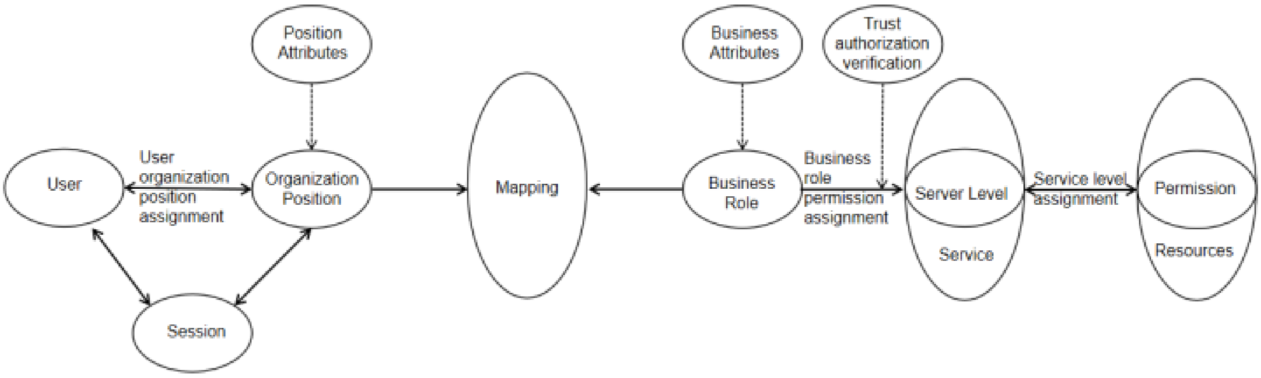

Fig.1. A fine-grained access control model combining attributes and trust

2.1. AT-RBAC model related definitions

Definition 1: model element definition

The following is the definition of AT-RBAC, a fine-grained access control model based on attributes and trust.

(1) Information resources. U is used to representing the entire set of users, and u is used to portraying a user in U.

(2) Session (S): Represents the collection of all sessions, which is the intermediary of the connection between the user and the organization position, and determines the scene in which the user is assigned the organization position.

(3) Organization Position (OP): Represents the collection of organizational positions, which refers to collecting users who hold positions in the unit.

(4) Business Role (BR): Represents a set of business roles, which refers to users who complete certain specific businesses.

(5) Service (Ser): The link between business roles and permissions is the only way to give users restrictions and collect service levels.

(6) Service level (Sl): The basic unit in the service, divided into multiple service levels according to the access level, is inherited.

(7) Permission (Per): Qualification for system resource access. A two-tuple composed of Action (Action) and Resource (Resource).

(8) Mapping (Map): Represents a collection of the relationship between organizational departments and business roles.

(9) Trust authorization verification: represents the process by which the subject verifies that the user is eligible to enter the service level.

(10) Trust Value: Indicates the user's qualification to enter the service level given by position attributes and business attributes. A trust value of 0~1,0 means no trust at all, and 1 means full trust.

(11) Trust threshold: Indicates the amount of service level that can be compared with the trust value. The system determines the user's authority level according to the trust threshold.

(12) Position Attributes (PA): Represents the characteristic information and objective description of the organization's position attributes.

(13) Business Attributes (BA): Represents the characteristic information and accurate description of the attributes of the business role.

Definition 2: attribute authentication

(1) Attribute screening

The model is based on the RBAC model and introduces the position attribute PA and business attribute BA to realize the certification of the organization's position and business role; the system screens users through the position attribute value and business attribute value and determines the missing position attribute value or business attribute value. The user does not have the authority to access resources, as shown in the attribute authentication table in Table 1. Attributes are dynamic. The more the salesperson who participates in the specific business in a business role, the higher the attribute obtained.

(2) Attribute value calculation

When the user accesses the system resources, it will provide the corresponding position attributes and business attributes. The system will decompose the user's position attributes and business attributes into more detailed evaluation factors for attribute value calculation.

Table.1. Attribute authentication

User	Position Attributes	Business Attributes	Attribute authentication result
User1	√	√	Success
User2	√		Failure
User3		√	Failure

Position attribute value calculation: The system delimits the level and assigns different position attribute values to users according to the classification of the position attribute, as shown in Table 2, the position attribute requirements.

Table.2. Job attribute requirements

Job Requirements	Position attribute value E_{K_1}	Trust value T_{K_1}
Minister	0.5	The user must meet one of the job requirements. Complete is 1, and incomplete is 0.
Deputy Minister	0.3	
Ministry staff	0.1	

Then calculate the current position attribute trust value as:

$$T_P = \sum_{k_1=1}^{n} E_{K_1} T_{K_1} \tag{1}$$

Among them, E_{K_1} represents the position attribute value, T_{K_1} represents the trust value, and the user who accesses the system must hold a position in the position requirement, then T_{K_1} =1; otherwise T_{K_1} =0. n represents the number of evaluation factors contained in the position attribute.

Job attribute value calculation: The system delimits the level and assigns different business attribute values to users according to the number of business attributes. Assuming that the system has a total of 3 businesses, as shown in Table 3, the business attribute requirements.

Table.3. Business attribute requirements

Business requirements	Business attribute value E_{K_2}	Trust value T_{K_2}
3 business	0.9	The user must meet one of the business requirements. Complete is 1, and incomplete is 0.
2 business	0.8	
1 business	0.7	

Then calculate the current business attribute trust value as:

$$T_B = \sum_{k_2=1}^{m} E_{K_2} T_{K_2} \tag{2}$$

Among them, E_{K_2} represents the business attribute value, T_{K_2} represents the trust value, and the user who accesses the system must serve as a business in the business requirements, then $T_{K_2} = 1$; otherwise $T_{K_2} = 0$. m represents the number of evaluation factors contained in the business attribute.

Definition 3: Trust evaluation mechanism

(1) Trust calculation

After the user completes the attribute authentication, the position attribute value and business attribute value will be provided to the system for trust calculation. User trust is one of the bases for measuring the user's resource access credibility, and it is updated and changed with the user's relevant information.

Calculate the trust of the current user as:

$$T_D = \alpha \sum_{K_1=1}^{n} E_{K_1} T_{K_1} + \beta \sum_{K_2=1}^{m} E_{K_2} T_{K_2} \tag{3}$$

Among them, $\sum_{K_1=1}^{n} E_{K_1} T_{K_1}$ represents the user's position attribute value, and $\sum_{K_2=1}^{m} E_{K_2} T_{K_2}$ represents the user's business attribute value; and α 、 β is the influence weight based on the position attribute and business attribute respectively. $\alpha + \beta$ =1.

The calculation of the trust degree is affected by the current trust degree and the historical trust degree at the same time, and the trust degree is affected by the context and time decay when it is transmitted, so the time decay function $H(t)$ is introduced to adjust the influence of the historical access behavior on the trust value calculation. The degrees are as follows.

Time decay function:

$$H(t) = \begin{cases} 1, & t = n \\ H(t-1) + \frac{1}{n}, & t < n \end{cases} \tag{4}$$

Calculate the historical trust of users as:

$$T_h = T_{D(t-1)} H_{(t)} \omega \tag{5}$$

Among them, $T_{D(t-1)}$ represents the trust of the last user, $H(t)$ represents the time decay function, and ω represents the weight of the system based on the user's various behavioral factors.

The overall trust of users is:

$$T_{all}(u) = (1-\gamma) T_D + \gamma T_h \tag{6}$$

γ is the historical trust degree influence rate. $\gamma \in [0,1]$The larger the value, the larger the proportion of trust in calculating the trust degree. When the user accesses the system for the first time, $T_{all} = T_D$.The overall trust degree is dynamic and will be based on the user's authority to interact with system resources Changes in size and historical performance.

(2) Trust authorization verification

When the user proposes to verify the trust authorization, the system will first check the user's overall trust value and then determine whether the user has the qualifications to enter the service level according to the overall trust level. For example, the trust level calculated by the system for user A this time is T_t, and T_1 is the critical value of the trust degree set by the system, then the trust level of user A is as shown in Table 4 (where α is a non-zero constant):

Table.4. Trust authorization verification

Overall trust value range	$(0,\ T_1)$	$[T_1,\ \alpha)$
Authorization verification result	Distrust	Trust

When user A's trust level is $T_t \in (0, T_1)$, the user trust authorization verification fails, and the system does not user A, then user A is not qualified to enter the service to obtain resources. When the user's trust level $T_t \in (T_1,\ \alpha)$, the user trust authorization verification succeeds, and user A is trusted, user A is eligible to enter the service to obtain resources.

2.2 AT-RBAC model access authorization mechanism

The authorization group of the AT-RBAC model can be represented by a five-tuple: $AT-RBAC = \langle U, R_p, R_b, P, T_{all}, C, O \rangle$, where U represents the user set, R_p represents the organization position role set, R_b represents the business role set, P is the access operation permission set, T_{all} represents the total trust of the user, and C represents the service. The trust threshold in the level, O represents the resource object authorized to access. Users $u_1(u_1 \in U)$, $u_2(u_2 \in U)$, and $u_3(u_3 \in U)$ are the department members $r_1(r_1 \in R_P)$, deputy ministers $r_2(r_2 \in R_P)$, and ministers of the organization department $r_3(r_3 \in R_P)$. The three of them also serve as salesmen. When requesting resource access, the system Service level authorization operations will be performed.

(1) Service level authorization

The system compares the overall trust level after the user authorization verification with the trust thresholds $c_1(c_1 \in C), c_2(c_2 \in C)$, and $c_3(c_3 \in C)$ in the service level to determine the access authority level. As shown in Figure 2, the trust level of the members of the organization department 1 $r_1(r_1 \in R_P)$is set to $t_1(t_1 \in T_{all})$, The trustworthiness of the deputy minister $r_2(r_2 \in R_P)$ is $t_2(t_2 \in T_{all})$ and the trustworthiness of the minister $r_3(r_3 \in R_P)$ is $t_3(t_3 \in T_{all})$. Assuming that three people are responsible for the same business, define the service level trust thresholds c_1 and c_2; and $c_2 > c_1$, set $t_3 > c_2 > t_2 > c_1 > t_1 > T_1$ at the same time; show in Table 5 for service levels Authorization table (where β is a non-zero constant).

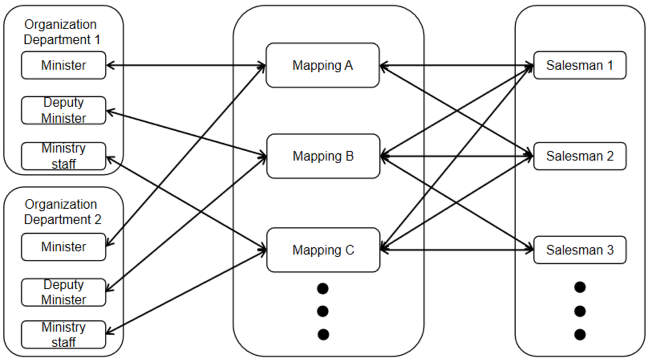

Fig.2. Mapping relationship between organizational positions and business roles

Table.5. Service level authorization table

Threshold range	$[T_1,\ c_1)$	$[c_1,\ c_2)$	$[c_2,\ \beta)$
Authorization level	Service level 1	Service level 2	Service level 3

when the trust of the department clerk is $t_1 \in [T_1,\ c_1)$, then he has the authority of service level 1; the trust of the deputy minister clerk is $t_2 \in [c_1,\ c_2)$, then he has the authority of service level 2. The trust of the minister clerk is $t_3 \in [c_2,\ \beta)$,then his Have service level 3 permissions.

As shown in Figure 3, each service level corresponds to a level of security level permission set. The upper service level can inherit the lower level. The ministerial clerk has the service level 3 permission, the deputy ministerial clerk has the service level 2 permission, and the member business The employee has only service level 1 authority.

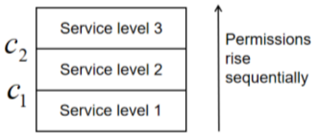

Fig.3. Assignment of service level restrictions

(2) Permission distribution

The permission set includes three permissions, namely: edit, share, and read, which are divided according to the level of permissions, as shown in Figure 4. To achieve dynamic mapping between business roles and permissions, trust in the service The design of the threshold realizes the dynamic authorization of permissions as the user's organizational position and business role changes. According to the user's trust after the trust authorization, the ministerial clerk has the editing permission, the deputy ministerial clerk has the sharing permission, and the departmental clerk There is only read permission, and at the same time the permission level is inherited, the upper-level permissions can inherit the lower-level permissions, as shown in Table 5. Figure 4 illustrates this dynamic permission granting process.

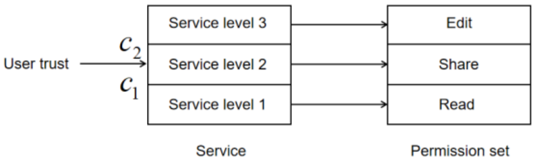

Fig.4. Service level and permission level mapping

Table.5. Permission assignment

Service level	Service level 1	Service level 2	Service level 3
Permission assignment	Read	Shared	Edit

2.3 AT-RBAC model access control mechanism

The access control mechanism for users to access system resources is shown in Figure 5.

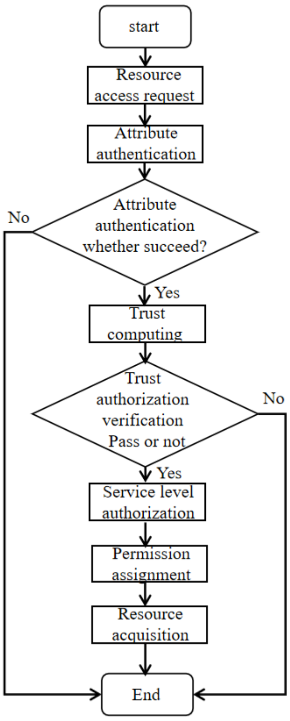

Fig.5. AT-RBAC model access control mechanism

The model's access control mechanism is as follows:

(1) The user enters the system to request resource access.

(2) The system authenticates the user's attributes; first, the system performs an attribute screening based on the user's position attributes, and business attributes to determine whether the user is eligible to enter the next stage of operation. If the user attribute screening is successful, the position attribute value will be performed And business attribute value calculation; if attribute authentication fails, the system refuses to provide services.

(3) Calculate the trust degree according to the user's position attribute value and business attribute value to obtain the overall trust degree A and determine whether the user is qualified to enter the service for resource interaction. If the overall trust degree A is greater than the trust degree threshold B, then The user is eligible to enter the service; if the overall trust level A is less than the trust level threshold B, the user is not qualified to enter the service.

(4) Based on the overall trust level T_{all} , the system compares with the thresholds $c_1(c_1 \in C)$ and $c_2(c_2 \in C)$ set in the service to determine the service level authorization operation.

(5) Determine the level of resource access permissions according to the user's service level.

3. Simulation analysis of fine-grained access control combining attributes and trust

This article uses Python 3.7 for simulation analysis.

Experimental environment: PC (Intel(R) Xeon(R) Gold 6148 CPU @ 2.40GHz, RAM 8GB, disk 256GB)

Simulation mainly analyzes from two aspects: the impact of changes in job attributes and business attributes on overall trust.

After the user enters the system, the system will first perform attribute screening. Only users who meet the requirements of position attributes and business attributes are eligible to enter the system's trust calculation. The user's overall trust value must meet the following conditions: the user's trust is OK. If the fluctuation occurs in a small range, that is, it fluctuates within the trust level set by the authority level. If the fluctuation range exceeds this range, it will cause the user's authority to change, posing a threat to the security of the system, which is not allowed by the system.

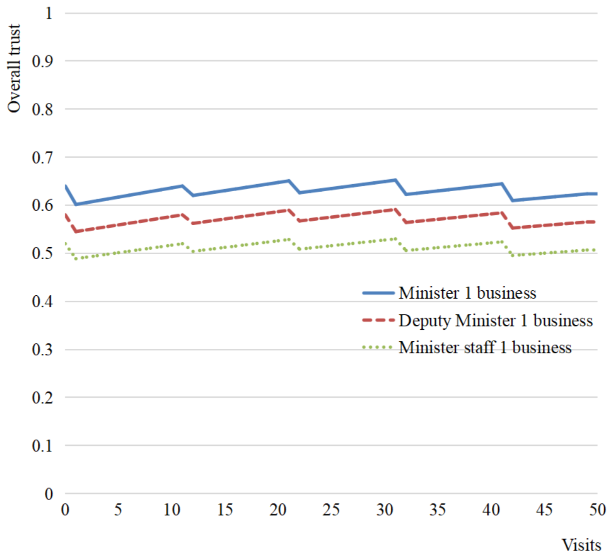

Fig.6. The impact of changes in job attributes on overall trust

3.1 The impact of changes in job attributes on overall trust

Set the three user positions as a minister, deputy minister, and department member, and they are responsible for 1 business at the same time. At this time, the position attribute values of the three are respectively 0.5, 0.3, and 0.1, and the business attribute values are all 0.7. The system sends out resource interaction applications, which are accessed 50 times, and the overall trust level change after each access is shown in Figure 6.

The position attribute of the three users is the only variable. The system calculates the user's corresponding overall trust degree according to the user's position. As shown in Figure 6, the overall trust degree is: Minister 1 business> Deputy Minister 1 business> Department Since the three members have entered the system for the first time, the total trust value of the first time is the current trust value of the three people. Starting from the second visit to the system, the calculation of the total trust value takes into account the historical trust value to the overall trust. The overall trust of the three people decreases. As the number of successful interactions increases, the overall trust of the three people increases. After every 10 interactions, the overall trust value of the user will decrease accordingly, preventing users from Too much overall trust has an impact on matching resource access rights. The overall trust of the three users fluctuates within a certain range, the trend remains at a stable level, and the maximum trust of users with low trust does not exceed the maximum of users with high trust. The minimum value of the trust level ensures that there will be no changes in the user's authority due to excessive trust level fluctuations, which proves the stability of the system and conforms to the actual situation.

3.2 The impact of changes in business attributes on overall trust

Set the user's position as the minister, which is responsible for 3 business, 2 business, and 1 business respectively. The position attribute value is 0.5, and the business attribute value is 0.9, 0.8, and 0.7 respectively. The user sends a resource interaction application to the system and accesses the system respectively. 50 times, the overall trust degree change after the visit is shown in Figure 7.

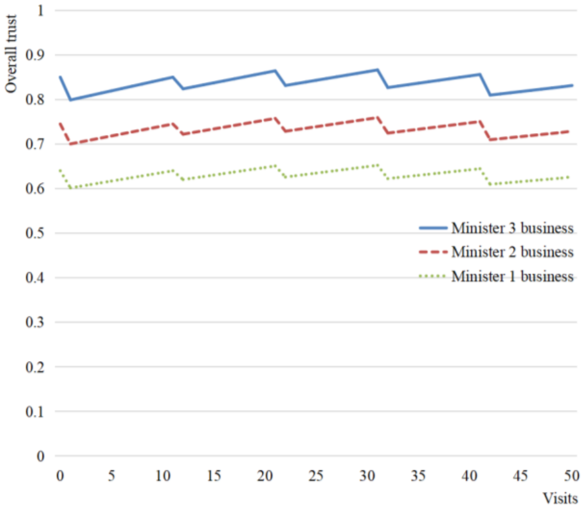

Fig.7. The impact of changes in business attributes on overall trust

The user's business attribute is the only variable. The system calculates the user's corresponding overall trust level according to the amount of business the user holds. As shown in Figure 7, the overall trust level is Minister 3 business> Minister 2 business> Minister 1 business. Although the three trustworthiness broken lines fluctuate, the overall trend is stable. The trustworthiness curve of the minister's 3 business is stable between 0.8-0.9, the trustworthiness curve of the minister's 2 business is stable between 0.7-0.8, and the minister is 1. The trust degree curve of the business is stable between 0.6-0.7, which ensures that the overall trust degree fluctuates within the trust degree area set by the authority level and will not cause changes in the authority and other operations that threaten the security of the system, which is in line with reality. Happening.

Because the actual business situation of the user may change each time the user accesses the system, this situation is simulated and simulated. The system sets the user position as the minister, and each time the user accesses the system, he assumes 3, 2, and 1 businesses randomly. The overall trust level shown in Figure 8.

Each time a user accesses the system, the system dynamically calculates the overall trust level according to the number of businesses the user assumes. As shown in Figure 8, the overall trust level of the user fluctuates greatly, but the overall trust level is stable in the range of 0.6-0.8. Internally, the trend is maintained at a stable level, and the system will match the corresponding resource access permissions according to the overall trust of the user's current access, which is in line with the actual situation.

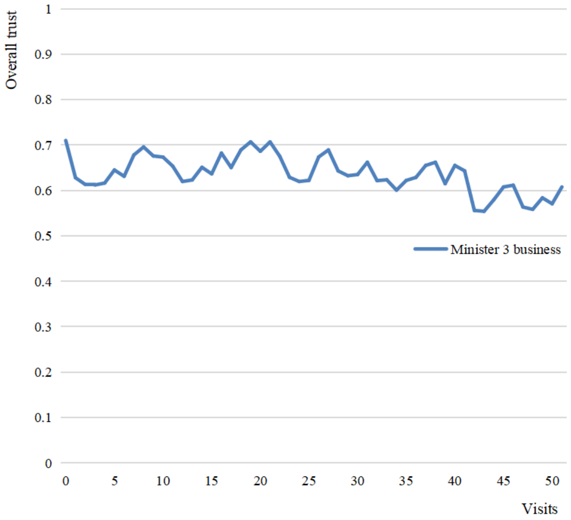

Fig.8. The impact of random changes in business attributes on overall trust

4. Comprehensive analysis of the model

4.1 Analysis of the characteristics of AT-RBAC model

Compared with other access control models, AT-RBAC has outstanding advantages. The comparison results are shown in Table 6. Based on the traditional RBAC model, the model divides roles into organizational positions and business roles to achieve organizational and business levels. The decoupling of the system achieves the purpose of fine-grained authorization of users; the introduction of the concept of service realizes the decoupling between business roles and authority operations; adding position attributes and business attributes as system constraints to achieve dynamic authorization of the system Establish a trust evaluation mechanism to dynamically analyze and evaluate users' behaviours. By calculating the user's overall trust value and determining the service level, ensures the dynamics of service level authorization and permission assignment and solves the traditional static RBAC model. Disadvantages of authorization. AT-RBAC has the dynamics and reliability that other models do not have through double-layer decoupling and double-layer security protection.

Table.6. Comparison of AT-RBAC with other models

Model	Double-layer decoupling between roles and permissions	System double-layer security protection	Dynamic authorization and fine-grained division of permissions
AT-RBAC	√	√	√
RBAC	×	×	×
Literature [13] Model	×	×	√
Literature [14] Model	√	×	√

4.2 Security analysis of AT-RBAC model

The AT-RBAC model is based on the traditional RBAC and uses attribute authentication and trust evaluation mechanisms to analyze the security of the access behaviour. If the user's position attributes or business attributes are not complete, the user will not be eligible to access the system; the user's overall trust value reflects the trustworthiness of the user. The trust value does not reach the critical trust value of the system, and the user cannot access the system; when the trust value does not reach the service level threshold, the user still cannot access the user, ensuring the user who has access to the system resources It will not pose a security threat to the system. Secondly, the model determines the service level according to the level of trust value and then determines the access rights to ensure the security of the system. Finally, the model organizes the positions and business roles and service levels by fine-graining. The introduction fully realizes the decoupling between roles and permissions and greatly enhances the security of the system.

5. Conclusion

Aiming at the characteristics of traditional access control that cannot achieve dynamic authorization and low security, this paper proposes a fine-grained access control model that combines attributes and trust, including model composition, element composition, access control process and policy formulation. Based on the traditional RBAC model, the model realizes the two-layer decoupling between roles and permissions by fine-graining roles into organizational roles, business roles, and the introduction of services while ensuring the fine-grained authorization of the system. Establishing the attribute authentication mechanism and the trust evaluation mechanism makes the system subject to double-layer security protection. The addition of position attributes and business attributes as elements of trust calculation realizes the dynamic authorization of the system to users who access system resources and improves the security of the system.

Acknowledgements

This work was supported by in part by Power Supply Service Center of State Grid Heilongjiang Electric Power Co., Ltd Under Grant No.5224131900A4, and The Fundamental Research Funds in Heilongjiang Provincial Universities No.135409602.

Reference

[1] Sandhu R,Coyne E J,Feinstein H L,ea al. Role-based access control models [J].IEEE Computer,1996,29(2):38-47

[2] Sandhu R,Bhamidipati V,Munawer Q.The ARBAC97 Model for role-based administration ofroles[J].ACM Trans on Information and System Security,1999,2(1):105-135.

[3] Gedare B,Rahul S.Hardware-enhanced distributed access enforcement for role-based access controls[C]// SACMAT'14.London,Canada:ACM,2014:5-16.

[4] Wouter K,Victor E.Sorting out role based access control.[C]//SACMAT'14.LONDER,Canada:ACM,2014:5-16.

[5] Cao Sheng, Yang Jie, Meng Qingchun. Research and design of system access security management based on PMI［J］. Computer Engineering, 2007, 33(24):141-143.

[6] SNYDER L. Formal models of capability -based protection systems[J]. IEEE Transactions on Computers,1981, 30(3):172－181.

[7] FERRAIOLO D F,KUHN D R. Role-based access controls ［C］/ /Proceedings of 15th NIST －NCSC. [s.l.]:[s.n.], 1992 : 554－563.

[8] SANDHU R,COYNE E J,FEINSTEIN H L,et al. Role -based access control models［J］. Computer, 1996, 29(2): 38－47.

[9] Cai Ting, Nie Qingbin, Ouyang Kai, etc. RBAC model based on role expansion [J]. Application Research of Computers, 2016, 33(3): 882-885.

[10] Liu Qingyun, Sha Hongzhou, Li Shiming, et al. A large-scale network access control method based on quantifying users and services [J], Chinese Journal of Computers, 2014, 37(5): 1195-1204.

[11] TAN Zhanjiang, TANG Zhuo, LI Renfa, et al. Research on Trustbased Access Control Model in Cloud Computing[C]//IEEE. Information Technology and Artificial Intelligence Conference (ITAIC), 2011 6th IEEE joint International, August 20-22, 2011, Chongqing, China. New Jersey: IEEE, 2011: 339-344.

[12] Ghafoorian M, Abbasinezhad-Mood D, Shakeri H.A Thorough Trust and Reputation Based RBAC Model for Secure Data Storage in the Cloud[C]//IEEE Transactions on Parallel and Distributed Systems. New York:IEEE ,2018:1-12.

[13] Gao Pengxiang. Research and design of dynamic access control model based on trust and role[D]. Tianjin University, 2014.

[14] Xiong Tianhong,Yu Yang,Lou Dingjun.Research on PRBAC Access Control Model in Workflow System[J].Journal of Applied Sciences, 2020, 38(05): 672-68105): 672-681

Jiaming Zhao was born in 1996.He is an M.S. candidate in the Qiqihar University. His research interests include image identification, Computer access control.

Jie Sun was born on December 26, 1973. He graduated from Northeast Electric University with a master's degree in electrical engineering in 1998. He has worked in science and technology for 16 years. He has participated in the scientific and technological project of Heilongjiang Electric Power Co., Ltd. and served as the project leader. He has published many high-level papers, and obtained 6 authorized invention patents. He has received 8 scientific and technological progress awards from Heilongjiang Electric Power Co., Ltd.

Xiaofeng Quan was born on April 28, 1974. He graduated from Northeast Electric Power University with a major in transmission line engineering in 1996. He has been engaged in the construction of transmission lines for 25 years and has rich experience in UHV and UHV management. He has participated in the construction of many 500 kV lines of the Three Gorges Project and participated in the UHV 800 kV Xizhe line as deputy project manager.

Hongbin Zhang was born on April 8, 1976. He graduated from Northwestern Polytechnical University in July 1996. He is currently the director, party committee member, and production branch secretary of the Fuyu County Electric Power Bureau. He has rich on-site practical operation capabilities.