Access Control Model of Industrial Control System Based on Multi-attribute Decision Making

Rui-Hong Dong, Tong-Tong Xu, and Qiu-Yu Zhang
(Corresponding author: Tong-tong Xu)

School of Computer and communication, Lanzhou University of Technology
No. 287, Lan-Gong-Ping Road, Lanzhou 730050, China
Email: xutongtong1007@163.com

(Received Aug. 5, 2020; Revised and Accepted Apr. 24, 2021; First Online Oct. 19, 2021)

Abstract

For solving the problem that the access rights cannot be dynamically adjusted when the environment and task status change in the industrial control system, and in the collaborative environment, there are many problems, such as permissions switching, permissions changing frequently, which make it inability to carry out fine-grained access control. This paper puts forward a kind of access control model based on multiple attribute decision-making. This model firstly evaluates multi-attribute factors such as environment, resources, and tasks in access control by introducing entropy TOPSIS and dynamically reflects the risk values in the process of access control. Then, based on the user's historical access record, an algorithm to calculate the user's trust value is proposed, which is used to adjust the user's access permission dynamically. Furthermore, the model integrates access control with the industrial control system's organizational structure and task attributes. Finally, a natural gas pipeline access control data set published by the University of Mississippi is used to verify the effectiveness of the proposed user trust value algorithm and entropy weight TOPSIS method for user trust value adjustment and task state decision. The experimental results show that the model can meet the requirements of dynamic permission adjustment and fine-grained access control in the industrial control system environment and has high security.

Keywords: Access Control; Dynamic Authorization; Entropy TOPSIS Method; Multi-attribute Decision-Making

1 Introduction

The normal operation of various types of tasks in industrial control systems requires the coordination of task allocation and resources of various departments. Operation users will constantly change, and the user's access rights should also change when the context in which the user accesses changes [3,8,11,15]. At the same time, the description of authority and authorization management in industrial control systems are affected by multiple attributes such as task execution environment and task state [10]. Due to the diverse types of tasks and complex processes in the industrial control system, its security control is relatively complex, so reducing the complexity of authorization is also an issue to be considered [2]. Therefore, the study of access control model based on multi-attribute decision making in industrial control system has been widely concerned by scholars and has very important theoretical research and application value.

In recent years, many researchers have made rich achievements in access control for industrial control system environments. For example, task-based access control model combines access rights with tasks to propose task-based access control model, which can solve the problem of dynamic assignment of permissions in workflow, but does not separate roles from tasks. The work-based Access Control (WBAC) model [21] can better meet the security requirements in the industrial control workflow environment, but it is weak in the ability of dynamic management authority. Team-based Access Control (TMAC) [1, 17]is extended from the aspect of user organization structure to improve the descriptive ability of user authorization and reduce the tedious degree of authorization in the process of user sub authorization. Although task-role-based access control model [19] can adapt to access control in task collaboration environment, it is static authorization and the permission inheritance method is not flexible enough. Moreover, it cannot real-time monitor users in the process of task execution, so it cannot meet fine-grained access control requirements in task collaboration environment. The basic idea of the Organization Based 4 Level Access Control (OB4LAC) model [16]is that in the authorization process, information related to roles and positions is utilized. However, the OB4LAC authorization is static, and the model's

constraints consist only of responsibility constraints and cardinality constraints, lacking finer grained constraints. The policy library of the Attribution-based Access Control model (ABAC) [6, 14] can be decentralized storage according to the actual situation, and can accurately describe the Access Control policy to realize fine-grained Access Control. However, in the system with a large number of subjects and resources, ABAC has too many access control rules. When the main body, resource attribute and environmental conditions increases, the number of rules will obviously increasing state, and an increase in the number of rules is likely to cause conflict strategy problem, at the same time the rapid increase of the number is likely to cause strategies library expansion, serious when even lead to normal operation of the system, is difficult to guarantee the system security and stability.

Literature [20] combined with ABAC integrates security level constraints into users, access behaviors and structured documents to realize multi-level access control mechanism of structured documents. It only conducts access control for a specific resource without considering the mutual constraints between tasks in workflow. The authorization method of the traditional access control model is still the authorization at the technical level. When the system is huge and complex, too many roles and permissions need to be managed, which increases the difficulty and complexity of authorization management, seriously degrades system performance, and even leads to authorization chaos [5, 9, 13]. The traditional access control model cannot be directly used in the workflow environment of industrial control systems, so a more fine-grained access control model is needed to divide specific tasks corresponding to specific resources, and realize dynamic control of permissions and real-time assessment of task risks.

Therefore, in order to solve the problems existing in the above research work, improve the flexibility of separation of responsibilities in the traditional access control model, and authorize the dynamic authorization in the process of task execution in real time. Combined with the industrial Control system, this paper presents a MATRBAC Model (Multi Attribute Task-based Access Control Model), which is more applicable to the fine-grained Access Control under the dynamic environment of the industrial Control system. The main contributions of this paper are as follows:

1) The proposed access control model based on multi-attribute decision making (MATRBAC) solves the problem that authorization is not flexible enough under the dynamic environment of industrial control system to realize real-time monitoring and management of users during task execution process.

2) In order to distinguish user credibility effectively and provide important basis for dynamic assignment of authority, an algorithm for calculating user trust value is proposed based on the user's historical access records.

3) By analyzing the data set of natural gas pipelines and comparing the characteristics of multi-attribute decision making under the industrial control system by linear weighting, analytic hierarchy process and Similarity by entropy Preference to an Ideal Solution, it is proved that the entropy TOPSIS method is more suitable for task state decision making under this environment.

The rest of the paper is organized as follows: Section 2 analyzes the factors associated with access control in the industrial control system and introduces the basic concepts of the MATRBAC model and the authorization process. Section 3 is the detailed design and introduction of two important modules of the MATRBAC model: the calculation of user trust value and the calculation of task transition risk value. In Section 4, we use a data set of a natural gas pipeline to analyze the effectiveness of the user trust value calculation method proposed by MATRBAC modeling, and compare the advantages and disadvantages of entropy weight TOPSIS algorithm and the same type of multi-attribute decision-making algorithm. Finally, the functional comparison and security analysis of MATRBAC model and other related access control models are carried out. In Section 5, the work of this paper is summarized.

2 Design of MATRBAC Model

2.1 Factors Related To Access Control in Industrial Control Systems

An abstract model of the factors associated with access control in an industrial control system is shown in Figure 1, which includes users, organizations, business roles, tasks, business processes, and business rules. In general, users belonging to an organizational structure perform assignments based on their jobs or business roles. Some tasks comprise business processes with special access control requirements. Many task rules and the user, environment, resource and other attributes involved in the process of task execution involve access control of various businesses. The access control model of industrial control systems should not only support finer grained access control but also ensure the separation of responsibilities and the principle of least privilege [12]. The specific attribute information involved in each factor in the access control process is analyzed below.

As shown in Figure 1 , the specific attribute information involved in each factor in the access control process mainly includes the following factors:

Task attributes: Include task type, task status, and task dependencies. From the perspective of access control, literature [4] can classify tasks in industrial control systems according to whether they can be inherited or whether they can be accessed passively: class P (Private), class S (Supervision), class

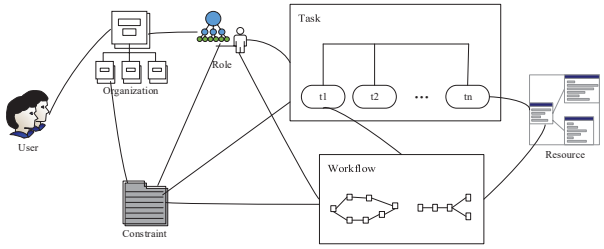

Figure 1: Abstract model of factors related to access control in an industrial control system

W (Workflow) and class A (Approval for activity). The task classification is shown in Table 1.

Table 1: Task classification in industrial control system

Pattern\Inheritance	non-inheritable	inheritable
active access	Workflow tasks(W)	approval tasks(A)
passive access	Private tasks(P)	Supervision (S)

Task states have four states: Ready, executing, suspended, and revoked. Task dependencies include the tasks that must be completed before the current task and the next task after the current task is completed.

User attribute: Subject specifically to a user in the industrial control system, each user has attributes associated with it, and these properties represent the main body status and characteristics of the included user ID, user roles, login name and password, the credibility of the user, system will be based on user history operation situation for real-time update, the concrete will be introduced in Section 4.2.

Resource attribute: [7] categorizes resources under the Internet of Things environment. In this paper, resources in industrial control systems are divided into device resources and data resources. The device can have the following attributes: device ID, device type, device location, device life, emergency alarm turn. Data resource attribute definition: device ID, information data, information data type, information data encoding, *etc.*

Operational attribute: Actions represent actions performed by the user on a resource, such as opening, closing, reading, writing, deleting, *etc.*

Environment attribute: In industrial control systems the environment refers primarily to the current time and date.

2.2 Structure of the MATRBAC

After the expansion of MATRBAC on the basis of ABAC and T-RBAC, the key improvements of the MATRBAC model are:

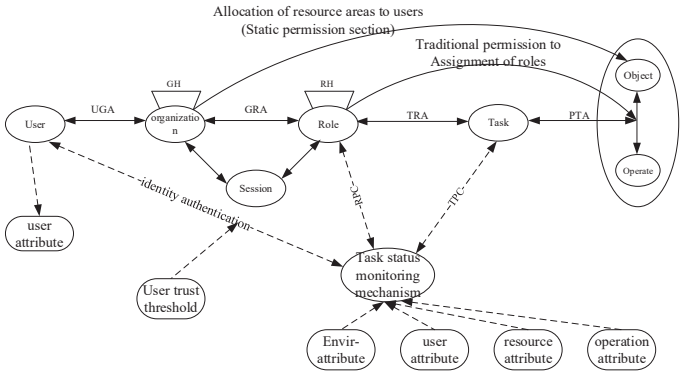

Figure 2: Structure of the MATRBAC model

1) Incorporating time and environmental constraints into the model so that the authority of the system is likely to change following the dynamic changes of time and environment;

2) The original four-tier structure of user-role-task-permission has been transformed into a five-tier structure of user-organization-role-task-permission. The introduction of organizational components on the basis of user and role components makes the model and industrial control application scenario more in line with reality. Moreover, when authorization is needed during the operation of the same task, the organization can automatically authorize through the assignment of roles, effectively reducing the pressure of administrator authorization;

3) A supervisory mechanism is added on the basis of roles and task components, which enhances the constraint correlation between roles and tasks and enhances the dynamic authorization between roles and tasks. Put an end to information leakage caused by malicious use of roles;

4) In the process of distributing the trust constraint is introduced into the dynamic permissions, the user's trust by user attribute and environmental attribute calculation, the user trust as a task execution status under dynamic decision-making authority of an attribute, along with the environment attribute, role attribute, time attribute and the task attribute calculation value at risk of the currently executing task, decision whether if the current task to terminate or permission to withdraw. The multi-attribute access control characteristics of the MATRBAC model are shown in Figure 2.

User: A user of the system or an actor of a task, and the set of users is denoted as $USERS$.

Organization: The corresponding organization department or position in the system, and the set of organization is denoted as $ORGANIZATION$.

Role: The permissions needed to implement a function or complete a business. A role is a set of permissions to perform a task. Users belonging to a role have the right and relevant permissions to perform the corresponding task. The set of roles is denoted as $ROLES$.

Session: Mapping between the organization and a subset of the set of roles that the organization owns. The organization $USES$ a session to activate a role, and the activated role has basic static permissions for parts of that role. A session is an active process of a role and sessions represents a set of $SESSIONS$.

Task: A logical unit of work that is indivisible and must be performed completely. A task is not a task in the real world, but an abstract representation of a class of tasks in the real world. Each task corresponds to a number of resource access permissions necessary to perform the task. The set of tasks is represented by $TASKS$.

Object: The content of a resource accessed by a user and also a protected object.

Operation: An executable program that is used by the user to perform operations on a resource (for example, read, write, update, delete).The set of all operations is represented by OPR. Any action the user performs on an object is completely defined within the permissions.

Permission: The collection of all permissions, represented by $PERMS$, is a combination of objects and operations.

2.3 Access Control Procedures for Models

In the model of MATRBAC access control described in this paper, the control of user rights assignment is realized dynamically through the interaction of user trust mechanism and task status supervision mechanism. The access control logic of the MATRBAC model is shown in Figure 3.

As shown in Figure 3, the authorization process of the MATRBAC access control model may be divided into the following five steps:

Step 1: The user logs in and issues an organization activation application. The organization controls the activation state of the user organization by judging the legitimacy of the user. Assign the organization when the user is legal, otherwise reject the user request.

Step 2: The organization assigns a role to the user. After the role is activated, it applies for permission to execute the task.

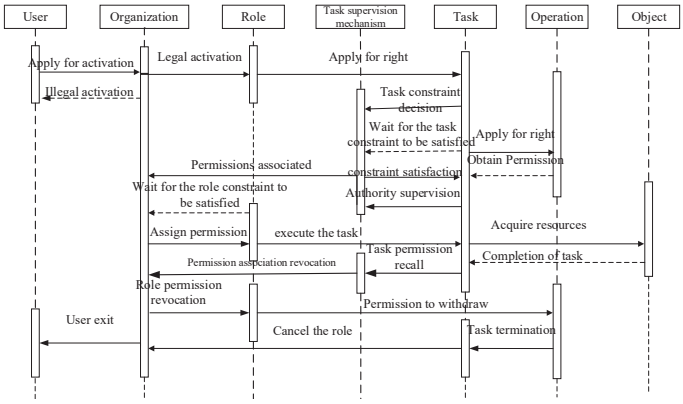

Figure 3: Access control logic of the MATRBAC model

Step 3: Task state supervision mechanism determines the task permission constraint. If the constraint does not meet, the task will be suspended and wait for the task to meet the constraint. When the task meets the constraint, the task will obtain the execution permission.

Step 4: Dynamically monitor whether constraints are met during task execution. If not, the task status monitoring mechanism revokes the permission and the task is suspended or terminated. If so, the task will continue to perform as normal until the permission is automatically revoked at the end of the task.

Step 5: After the normal completion of the task, reclaim the role permission, revoke the role task association, revoke the permission organization association, and the user exits.

3 Implementation the MATRBAC Model

The dynamic authorization and fine-grained authority management of the MATRBAC model is realized through the task status supervision module and the user trust determination module. Multi-attribute decision making is an important application in task state monitoring module. A user trust value determination algorithm is proposed, which can distinguish the user credibility effectively by the user's historical operation record and reputation record, and has the time attenuation factor. The following will describe in detail the multi-attribute decision is the task status monitoring module and the user trust determination module.

3.1 Task Status Monitoring Module

Task status supervision mechanism is the user activated after a character is in the process of performing tasks on the supervision and management of a function module, through the user properties, environment, resources, task

attribute of the constraints of dynamic judgment, the role of permissions granted to and revoked the real-time dynamic monitoring, can strengthen the roles are endowed with the strength of the rules to follow, improve the security in the process of task execution. By introducing the task state dynamic management module to decouple role authorization and role behavior, the system's ability to resist malicious attacks can be enhanced.

The factors affecting the industrial control system environment analyzed in Section 2.1 include user attribute, environment attribute, resource attribute and task attribute. The multi-attribute decision making algorithm is used to calculate the risk value of task state. Finally, a reasonable threshold value is obtained through systematic testing. If the calculated risk value is larger than the set threshold value, the execution state of the task will be changed, and after risk screening, the task state can enter the ready state and continue. Task status monitoring mechanism is shown in Figure 4. Its core components include task status monitor, authorization structure, policy decision point, policy information point, *etc.*, which are defined as follows:

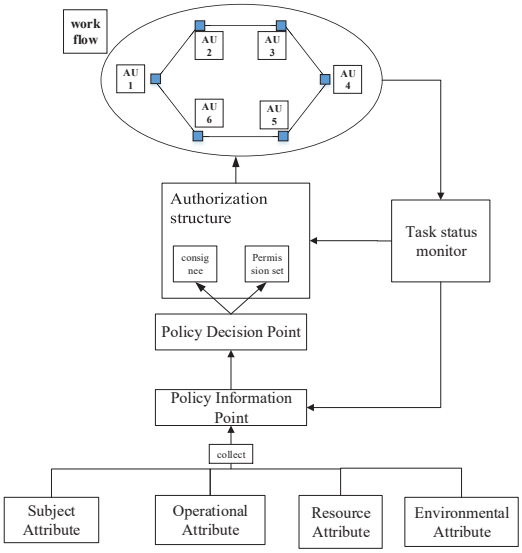

Figure 4: Task status monitoring mechanism

Task status monitor: Real-time monitoring of task execution state, acquisition of current task attributes, and calculation of current task risk value. If the risk value is greater than the set threshold value, the authorization structure can be suspended or revoked directly, and the current environment attributes, user attributes and operation attributes can be returned to the decision information point.

Authorization structure: It refers to the set of resources required to complete a task or operation, including the entrusted user and the operation set. The entrusted user is the set of personnel to complete the current task or operation, and the operation set refers to the set of permissions required to complete this part of operation.

Policy Decision Point: It refers to the attribute information provided to the policy information point, gives the permission decision, and creates the authorization structure.

Policy information points: Collect and save key attribute information, including principal attribute, action attribute, environment attribute, and resource attribute.

Operation steps of task status monitoring mechanism:

Step 1: Set the subject attribute, operation attribute, resource attribute and environment attribute in advance.

Step 2: Policy information points collect, filter, and store these attribute values.

Step 3: The policy decision point requests relevant attribute information from the policy information point according to the task attribute.

Step 4: The policy decision point creates the authorization structure through the collected attribute information and task attribute information.

Step 5: Authorize the structure to implement the action on the task.

Step 6: The task status monitor monitors the task status in real time.

Step 7: If the task status risk value is greater than the set risk threshold, the task status monitor will adjust, suspend or revoke the state of the authorization structure as the case may be, and send the collected attribute information to the policy information point to provide the basis for the next decision.

Step 8: The authorization structure is revoked immediately after it completes the task.

Common multi-attribute decision making algorithms that can be used to calculate task risk are

1) Simple weighting (SAW);

2) AHP;

3) Entropy weight TOPSIS.

The simple weighting algorithm is simple and easy to understand, but it requires that the values of all attributes are constant and can be compared, and that there is no important complementarity between attributes. Considering that the attributes related to access control in industrial control systems are complementary, and that this method cannot reflect the prominent influence of some attribute indexes, thus resulting in the distortion of evaluation results, this paper does not adopt this method. A comparison of the three methods is given in Section 4

with an example. In this paper, TOPSIS method is used to calculate the risk value of task status.

TOPSIS (Technique for Order Preference by Similarity to an Ideal Solution) [5] was first proposed by C.L.Wang and K.oon in 1981. TOPSIS is a sorting method based on the proximity of a finite number of evaluation objects to the ideal target, and evaluates the relative merits of existing objects. The basic principle is to sort the evaluation object by detecting the distance between the evaluation object and the optimal solution and the worst solution. If the evaluation object is the closest to the optimal solution and the furthest away from the worst solution, it is the best.Otherwise it's not optimal. Among them, each index value of the optimal solution achieves the optimal value of each evaluation index.Each index value of the worst solution reaches the worst value of each evaluation index. The process of TOPSIS Algorithm 1 is as follows: A positive ideal solution is a hypothetical optimal case in which each attribute value achieves the best of the alternatives. The negative ideal solution is the worst imaginable, with each attribute value reaching the worst of the alternatives. The ranking rule of schemes is to compare alternatives with ideal solution and negative ideal solution. If one of the alternatives is most close to ideal solution, but at the same time far away from negative ideal solution, the scheme is the best scheme among alternatives. The evaluation criteria of positive ideal solution and negative ideal solution are generally divided into three types:

Algorithm 1 TOPSIS

1: Begin
2: Initialize the Raw data set R and the weight of each index $w = w_1, w_2, ..., w_n$
3: The index attributes in the original data set are converted into B in the same direction.
4: Set up the weighted normalization matrix Z.
5: **for** each $z_j \in Z$ **do**
6: The z_j dimension of the optimal scheme $Z^- \leftarrow A^+$ Element minimum
7: The z_j dimension of the optimal scheme $Z^+ \leftarrow A^-$ Element maximum
8: **end for**
9: **for** each $z_j \in Z$ **do**
10: Degree of proximity between z_j and the optimal scheme d_i^+. (Formula 7)
11: z_j proximity to the worst d_i^-. (Formula 7)
12: Degree of closeness between z_j and the optimal scheme C_i. (Formula 8)
13: **end for**
14: Sort by size C_i
15: TOPSIS evaluation results of each data sample

Very small indicators: the smaller the expected index value is, the better (such as morbidity and mortality).

Intermediate index: the expected index value should be neither too large nor too small, and the appropriate intermediate value should be the best (such as the PH value of water quality assessment).

Interval index: The best value of expected index should be in a certain interval (such as body temperature). The ideal solution of dynamic decision making based on multi-attribute access control authority in industrial control system belongs to intermediate index.

Assumption in the industrial control system standard values for a property, as an index of the maximum possible value, m as an index of possible value of the minimum value, then the properties of expectations index value computation formula is as follows:

$$x' = \begin{cases} 2\frac{x-m}{M-m}, & m \le x \le \frac{1}{2}(M+m) \\ 2\frac{M-x}{M-m}, & \frac{1}{2}(M+m) \le x \le M \end{cases} \quad (1)$$

In this article for each attribute weights calculation using the entropy weight method, entropy method is more objective and can better explain the results, the use of information between the variability (*i.e.*, diversity) for empowerment, but need to have some sample size when using this method, through the sample to determine the weights, as determined by a weight on the analysis of the new things. In the specific application process, the entropy weight method calculates the entropy weight of each index according to the variation degree of each index by using the information entropy, and then modifies the weight of each index through the entropy weight, so as to obtain the more objective index weight.

Step of task status risk value calculation:

Step 1: Analysis task status by the risk value by the user attribute,environment attribute, multiple attribute decision factors such as task attribute, attributes expressed with Q, build property set:Q. The task set to be analyzed is represented by P. The attribute of task $Pi$for the Qj corresponding attribute values expressed in rij $(i = 1, 2, ..., m; j = 1, 2, ..., n)$.

Step 2: Each attribute value of each task to be analyzed is represented by rij to obtain the multi-attribute decision matrix R:

$$R = (r_{ij})_{m\times n} = \begin{bmatrix} r_{11} & r_{12} & \cdot & \cdot & \cdot & r_{1m} \\ r_{21} & r_{22} & \cdot & \cdot & \cdot & r_{2m} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ r_{n1} & r_{n2} & \cdot & \cdot & \cdot & r_{nm} \end{bmatrix} \quad (2)$$

Step 3: The weight of each attribute is calculated by entropy weight method: Calculate the proportion of the attribute value of the i-th sample method in the j-th attribute p_{ij}:

$$p_{ij} = r_{ij} / \sum_{i=1}^{m} r_{ij} \quad (3)$$

Calculate the entropy value e_{ij} of the j-th index:

$$e_{ij} = -k \sum_{i=1}^{m} p_{ij} \cdot \ln p_{ij} \tag{4}$$

with $k = 1/\ln m$. Calculate the entropy weight of the j-th index w_j:

$$\omega_j = (1 - e_j) / \sum_{j=1}^{n} (1 - e_j) \tag{5}$$

The relative importance of each factor is expressed as $w_1, w_2, ..., w_n$ represents and meets the normalization condition:

$$\sum_{j=1}^{m} w_j = 1 \tag{6}$$

Step 4: The decision matrix $R = [r_{ij}]_{m*n}$was standardized to obtain the matrix $B = [b_{ij}]_{m*n}$.

Step 5: Establish the weighted standardized matrix $Z = [z_{ij}]_{m*n}$, with $z_{ij} = b_{ij} w_j$.

Step 6:] Determine the positive and negative ideal solutions $A^+ = (z_1^+, z_2^+, ..., z_n^+)$and $A^- = (z_1^-, z_2^-, ..., z_n^-)$, $A^+$and A^-represent the most ideal and the least ideal solutions respectively. Where:

$z_j^+ = \max z_{ij}, z_j^- = \min z_{ij} \quad j \in$ Efficiency measure

$z_j^+ = \min z_{ij}, z_j^- = \max z_{ij} \quad j \in$ Cost type measure

Step 7: Compute the Euclid distance d_i^+ and d_i^+ between each solution and the positive and negative ideal solution:

$$d_i^+ = \sqrt{\sum_{j=1}^{m} \left(z_{ij} - z_j^+\right)^2}, d_i^- = \sqrt{\sum_{j=1}^{m} \left(z_{ij} - z_j^-\right)^2} \tag{7}$$

Step 8: Calculate the paste progress of each task sample and positive ideal scheme:

$$C_i = \frac{d_i^+}{d_i^+ + d_i^-} \tag{8}$$

Step 9: According to the characteristics of the system attribute value, set the risk threshold and compare it with C_i. If C_i is less than the set threshold, it will be judged as a risk task and the task-related permissions will be adjusted.

3.2 User Credibility Determination Module

When a user is granted an organization and the corresponding role, he/she already has some basic permissions, but during the execution of the task, Is granted other advanced permissions according to the different tasks. In order to prevent the abuse of permissions in the process of task execution, every time the user opens a task, a judgment is made on the credibility of the user, and then compared with the preset threshold, so as to determine whether the user has the authority to execute the task.

User credibility is related to three parts:

1) Historical credibility,

2) Reputation and credibility,

3) Time attenuation factor.

Historical trust value calculation: When the user requests to access system resources, the system will obtain the user's operation record and record it in the database. Firstly, the historical operation record of the user is obtained. The number of legal operations of the user and the resource is denoted as n. The illegal interactive access times of users are recorded as m, V_{ni} represents the trust value after each legal access, and V_{mi} represents the trust value after each illegal access. When the user accesses legally, $n = n + 1$, Otherwise, $m = m + 1$, V_k is used to represent the trust value after the end of the current access behavior, which can be calculated according to Formula (1).

$$V_k = \frac{\sum_{i=0}^{n} V_{ni}}{n} - \frac{\sum_{i=0}^{m} V_{mi}}{m} \tag{9}$$

Calculate the behavior trust value before the current access V_k', and then calculate the actual behavior trust value V_h based on the current and previous trust values.

$$V_h = \frac{V'k + V_k}{2} \tag{10}$$

When a user accesses the resources in the cloud platform for the first time, due to the lack of historical data, it is impossible to accurately calculate the actual trust value of the user. So his actual behavioral trust value is equal to the current behavioral trust value.

$$V_h = V_k \tag{11}$$

To sum up, the actual trust value of the user's historical behavior is:

$$V_h = \begin{cases} \frac{V'k + V_k}{2}, & (\text{Non} - \text{first access}) \\ V_k, & (\text{For the first time to access}) \end{cases} \tag{12}$$

Reputation is a measure of a user's trust by the other. In a system, the user is not only the visitor of the resource but also the owner of the resource. Access is a two-way process, during which mutual trust values are formed. The trust value cannot be passed, but by listening to the wishes of another user, the trust value can be adjusted to better meet the requirements of the system. It is not comprehensive to control the user's behavior by relying solely on the historical trust value, and it may face the problem of malicious access. Therefore, the trust of the third party is increased to monitor the user's behavior, that is, to conduct the trust evaluation based on

the evaluation information of the user by others. When user u accesses other resources, other resources also have a trust value store for user u. Then the reputation trust value of the user is:

$$V_{ck} = \frac{\sum_{k=0}^{q} c_k}{q} \tag{13}$$

Where, V_{ck} represents the reputation trust value of the user, C_k represents the trust value of the third party to the current user, and q represents the number of the given third party to the user. Trust value decays over time: If a user has not accessed a resource for a long time, his trust value for that resource also decays over time. The trust value plus the time decay factor, the trust value between people in the real world will be disconnected for a long time and the trust value will decrease with time. The decay rate of the trust value is not constant and is related to time. The time decay factor is expressed by a(t), and the calculation formula is:

$$\mathrm{a(t)} = e^{-k(t-t_0)} \tag{14}$$

Where k is the set attenuation coefficient, t is the current time, t_0 is the last access time.

According to the above analysis, the reliability calculation formula of users is as follows:

$$\mathrm{T}\left(u_t\right) = \mathrm{a(t)}\left(\alpha V_h + \beta V_{ck}\right) \tag{15}$$

Where $\alpha?\beta$ are the weights of historical trust value and reputation trust value respectively, the value range of and is [0,1], and $\alpha + \beta = 1$.

4 Experiment and Safety Analysis

4.1 Introduction of Experimental Data Set and Experimental Environment

The data set used in this experiment is the data set obtained from the laboratory-scale natural gas pipeline system of the University of Mississippi [18]. There are a total of 274,628 records in the data set, of which 210,528 records have incomplete characteristics. If the missing data is filled with average value or other methods, it is difficult to reflect the real state of the system for the multi-attribute decision making scheme studied in this paper. In view of this, records with missing features and attributes that are not relevant to the access control schemes studied in this article are removed, and some attributes related to access control mentioned in this article are appropriately added based on the results of the data set. The dataset contains four types of attacks: response injection, detection, distributed denial of service injection, and command injection. Response injection is divided into simple malicious injection (NMRI) and complex malicious injection (CMRI). Command injection can be divided into malicious status command injection (MSCI), malicious parameter command injection (MOCI) and malicious functional code injection (MFCI) attacks. Detect attacks to collect control system network information, draw network architecture, identify equipment characteristics, such as manufacturer, model, database information, *etc.* Table 2 lists the access-control-related attribute selected for this paper and their descriptions.

Table 2: Access control-related attribute and descriptions selected for this article

Attribute	Descriptions
address	MODBUS slave device workstation address
taskcode	Function code
usertrust	User trust value
time	Time to perform tasks
PIDgain	PID gain
PIDresetrate	PID reset rate
PIDrate	PID rate
pressure	Pressure measurement
deadband	PID dead band
cycletime	PID cycle time
cmdresponse	Command or response
Attack category	Category of attack
specific result	Specific attack

The experimental hardware platform was Intel(R) Core(TM) I5-7300HQ CPU, 2.50ghz, and 8GB of memory. The experimental software platform is: operating system bit windows 10, development tool is Python 3.7.

4.2 Experimental Methods and Results Evaluation

Dynamic adjustment of user trust value: given two users, the initial trust value is 0.5, and the trust time decay coefficient is 0.2. The change of trust value is calculated in the interaction process of 50 tasks selected respectively to see whether it is consistent with the actual situation. Figure 5shows the change in trust values between the two users over 50 tasks. As can be seen from Figure 5, at the

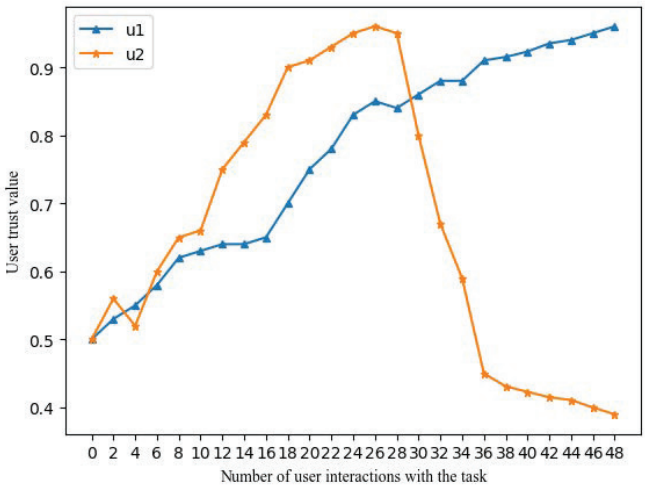

Figure 5: Fluctuation curve of user trust value

beginning, the trust values of users u1 and u2 both showed

a fluctuating rising trend. u1 rose more slowly than u2, but u2's trust value steadily rose, and u1 first gained the highest trust value in the interaction. From the 27th task, u2 trust value gradually decreased. According to the data analysis, u2 trust value decreased rapidly due to the influence of time decay factor 30 days between the 27th task and the 28th task. It conforms to the attenuation law of fast and slow decline of trust value. The experiment shows that the proposed method is effective. This method can accurately reflect the influence of user's behavior on the trust value under different task scenarios.

Calculation of task status risk value: In this experiment, 1000 pieces of data from the above attributes and corresponding data set were selected for risk value calculation by simple weighting method, analytic hierarchy process and entropy weight TOPSIS method respectively. The data includes both the normal and the attack. This paper evaluates the three multi-attribute decision making algorithms in terms of the degree of differentiation of calculated risk values, and then selects the algorithm more suitable for the system's multi-attribute access control risk value calculation. The matching degree between the high risk state calculated by entropy method, analytic hierarchy process and TOPSIS method and the actual situation was compared respectively. The lower the value of risk calculated under normal circumstances, the better. The higher the value of risk calculated under abnormal circumstances, the better. The entropy weight method is used to calculate the weight points of 11 attributes, as shown in Figure 6. As can be seen from Figure 6, the weights of the 11 attributes selected in this paper calculated by information entropy method are respectively 0.01359, 0.02313, 0.2604, 0.1142, 0.10146, 0.0752, 0.048, 0.0634, 0.1536, 0.0427 and 0.10432. Among them, the weight of user trust value is the largest and the weight of address is the smallest, which conforms to the actual rules in the system.

The 1000 samples were calculated according to the simple weighting method, analytic hierarchy process and entropy weight TOPSIS method, and then sorted into 20 small samples to calculate their mean value, as shown in Table 3. Among them, samples 17-20 were samples with abnormal task status. It can be seen from the table that the task risk value calculated by simple weighting method and hierarchical analysis is not clearly distinguished due to the small difference in sample data, while the entropy TOPSIS method can be clearly seen in the table that the risk value changes significantly between samples 16 and 17. In order to show the risk differentiation degree of the three algorithms in the system data set more clearly, the comparison diagram of the risk differentiation degree of simple weighting method, analytic hierarchy process and entropy weight TOPSIS in this sample is drawn, as shown in Figure 7. It is obvious that the TOPSIS method has a high degree of distinction. It can be seen from Figure 7 that the entropy weight TOPSIS method changes significantly in the risk values of sample 16 and sample 17 compared with the other two algorithms, which can intuitively reflect the attacked samples of the system, indicating that the entropy weight TOPSIS is more in line with the multi-attribute decision making of task risk under the system environment.

Table 3: Three algorithms respectively calculate the mean risk of their corresponding samples

Sample	SLW	AHP	Entropy TOPSIS
Sample1	13.333	13.960	0.976
Sample2	13.236	13.873	0.972
Sample3	13.229	13.570	0.96
Sample4	13.206	13.533	0.944
Sample5	13.179	13.313	0.942
Sample6	12.996	13.168	0.929
Sample7	12.839	12.987	0.89
Sample8	12.774	12.878	0.887
Sample9	12.760	12.675	0.857
Sample10	12.746	12.636	0.844
Sample11	12.723	12.431	0.839
Sample12	12.660	12.130	0.829
Sample13	12.644	12.091	0.826
Sample14	12.630	12.067	0.817
Sample15	12.612	12.032	0.812
Sample16	12.584	12.001	0.803
Sample17	11.683	11.700	0.426
Sample18	11.349	11.697	0.093
Sample19	11.023	11.601	0.076
Sample20	11.005	11.389	0.075

4.3 Security Analysis of the Model

In general, access control models in an industrial control system environment must meet the following requirements:

1) Fine-grained access control.

2) With stronger expansibility.

3) The authorization process is simple.

4) Active and passive access control coexist.

5) Dynamic detection and risk quantification of users' behaviors.

The model of MATRBAC achieves finer grained access control. The traditional role-based access control model assigns permissions to the role level. The access control model based on the task role correlates the task with the role, and the permission assignment realizes the more granular assignment of the permission at the task level to some extent. Following the role based access control model, MATRBAC retains the access control mechanism of the task role-based access control model, In addition, in

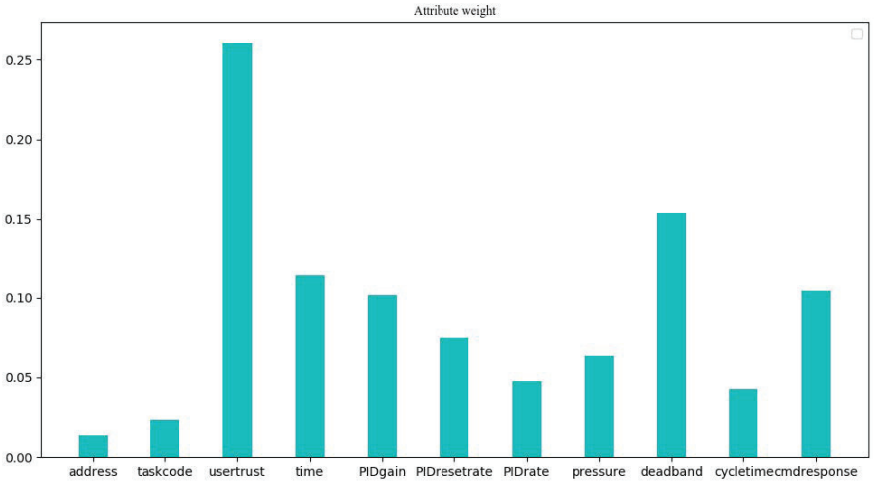

Figure 6: Weight distribution of 11 attributes in the dataset

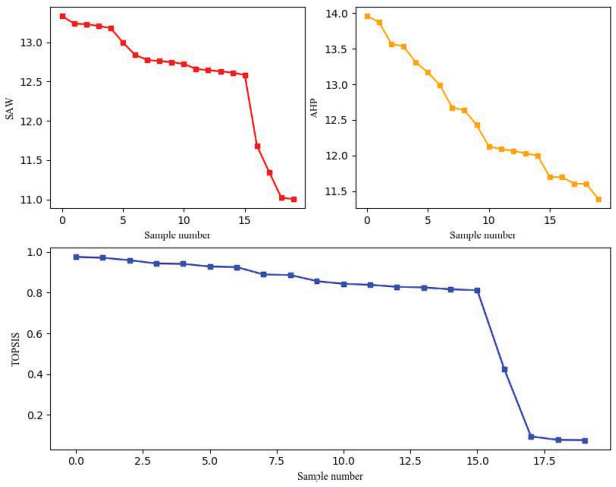

Figure 7: Weight distribution of 11 attributes in the dataset

the process of task execution, by collecting and saving key attribute information, including subject attribute, operation attribute, environment attribute and resource attribute, task execution is subject to environmental constraints, which effectively increases the ability of access control model to describe fine-grained constraints. The entropy weight TOPSIS is introduced to evaluate the risk of task state, which can adjust the access control strategy in real time according to the specific task running state and make access granularity finer.

The MATRBAC model is more scalable. The introduction of organization and role in the MATRBAC model is more consistent with the structure of industrial control system in reality, especially the classification of tasks, making different types of tasks subject to different access control strategy constraints and more consistent with the multi-task scenario in industrial production.

The MATRBAC model simplifies the authorization process. Through the introduction of organization, all and part of authority inheritance in the organization structure can be realized through the association relationship between organization and role and the hierarchical inheritance relationship between organization and role when the roles need to delegate authority to complete the same task. Permissions can change quickly through the association between the organization and the role, without the need for administrators to operate alone, and the introduction of the organization reduces the complexity of the authorization process.

The MATRBAC model integrates active and passive access control. The classification of tasks shows that the MATRBAC model is an active access control task for type A activity approval task and type W workflow task. Private tasks of class P and supervisory tasks of class S belong to passive access control. The MATRBAC model distinguishes between active and passive access control by the task.

The MATRBAC model integrates the determination of the user's trust value. Through the user's historical access record, the evaluation record of other resources to the user. And the user's access time interval to a specific resource, the user's trust value is calculated comprehensively. The user's trust value is an important reference index for assigning roles and tasks to users. As well as one of the indexes for task status risk assessment. This design makes the assignment of permissions more reasonable and reflects the dynamic assignment strategy of MATRBAC access control model to permissions.

4.4 The Comparison of the Model with Other Models

Table 4 provides a comprehensive comparison and analysis of the MATRBAC model introduced in this paper and the existing access control model, In the table, "$\surd$" means that the model proposed in the literature can meet the requirements of a security feature; " $\times$ " means that the model proposed in the literature cannot meet the requirements of a security feature.

As shown in Table 4, the access control model MATRBAC in this article provides better security features and more functional attributes compared to other relevant access control models. Therefore, the MATRBAC model is more applicable to the industrial control system environment.

5 Conclusions

This paper presents a MATRBAC model based on multi-attribute decision making. This model introduces the concept of organization and can adapt to the hierarchical structure of industrial control system and reduce the complexity of authorization effectively. Constraints such as subject attribute, operation attribute, resource attribute and environment attribute are added to enhance the ability of describing permissions. An algorithm for calculating user trust value by using user history access record is proposed to improve the model's adaptability and security to permissions. The multi-attribute decision making algorithm is applied to the task execution, and the risk value of the task is calculated in real time through the change of each attribute value during the task execution. By using user trust value judgment module and task supervision module, the authority can be dynamically adjusted during task execution, which can adapt to the special situation to achieve both coarse granularity and fine granularity. The experiment demonstrates the use of entropy weight TOPSIS method for multi-attribute decision making is more discriminative than that of simple weighting method and analytic hierarchy process, which can more intuitively show the difference between normal task and risk task, and demonstrate the availability of MATRBAC model for authority dynamic adjustment in industrial control system environment. Compared to other access control models, MATRBAC has more security features and extensibility.

Acknowledgments

This study was supported by the National Science Council of Taiwan under grant NSC 95-2416-H-159-003. The authors gratefully acknowledge the anonymous reviewers for their valuable comments.

References

[1] F. T. Alotaiby and J. X. Chen, "A model for team-based access control (TMAC 2004)," in *International Conference on Information Technology Coding and Computing*, pp. 450–454, Sep. 2004.

[2] S. Y. Belim and N. F. Bogachenko, "User authorization in a system with a role-based access control on the basis of the analytic hierarchy process," *Dynamics of Systems Mechanisms and Machines*, vol. 66, no. 08, pp. 1–5, 2017.

[3] N. Chistokletov and Y. Vavilin, "Safety management system of machine-building production," *Engineering Review*, vol. 38, no. 2, pp. 226–231, 2018.

[4] K. Haefner, B. Bezawada and I. Ray, "Securing home IoT environments with attribute-based access control," *Proceedings of the Third ACM Workshop on Attribute-Based Access Control*, vol. 86, no. 34, pp. 43–53, 2018.

[5] X. Hei, R. Akkaoui and C. Guo, "RBAC-HDE: On the design of a role-based access control with smart contract for healthcare data exchange," in *IEEE International Conference on Consumer Electronics - Taiwan (ICCE-TW'19)*, pp. 156–163, Sep. 2019.

[6] D. R. Kuhn, V. C. Hu and D. F. Ferraiolo, "Attribute-based access control," *Computer*, vol. 48, no. 2, pp. 85–88, 2015.

[7] E. S. Lee, H. S. Shih, H. J. Shyur, "An extension of topsis for group decision making," *Mathematical Computer Modelling*, vol. 5, no. 7, pp. 801–813, 2007.

[8] X. Lian, Y. Chen and D. Yu, "Exploring shodan from the perspective of industrial control systems," *IEEE Access*, vol. 99, no. 1, pp. 1–1, 2020.

[9] S. Long and L. Yan, "Racac: An approach toward rbac and abac combining access control," in *IEEE 5th International Conference on Computer and Communications (ICCC'19)*, pp. 16–25, Nov. 2019.

[10] S. Lu, F. A. Bhuyan and R. Reynolds, "A security framework for scientific workflow provenance access control policies," *IEEE Transactions on Services Computing*, vol. 99, no. 32, pp. 1–1, 2019.

[11] S. Mikko, D. Gregory and P. Seppo, "Toward a unified model of information security policy compliance," *MIS Quarterly*, vol. 42, no. 3, pp. 285–311, 2018.

[12] S. Oh and S. Park, "Task-role-based access control model," *Information Systems*, vol. 23, no. 6, pp. 533–562, 2003.

[13] B. Ou, S. Y. He and X. Liao, "Access control model of role matching in distributed workflow environment," *Computer Science*, vol. 45, no. 7, pp. 129–134, 2018.

[14] D. Servos and S. L. Osborn, "Current research and open problems in attribute-based access control," *ACM Computing Surveys*, vol. 49, no. 4, pp. 1–45, 2017.

[15] J. Shevchenko and David, "Joint management systems for operations and safety a routine-based perspective," *Journal of Cleaner Production*, vol. 194, no. 1, pp. 635–644, 2018.

Table 4: Comparison of security features

feature\Model	$RBAC^{[7]}$	$T-RBAC^{[15,24]}$	$ABAC^{[17,18]}$	$WBAC^{[12]}$	$AMAC^{[19]}$	$MATRBAC$
role concepts	√	√	√	√	√	√
task concepts	×	√	√	√	×	√
organizational concepts	×	×	×	×	×	√
Supporting environment	×	×	√	×	√	√
Support the tense	×	×	√	×	√	√
role units	√	√	√	√	√	√
task units	×	√	×	√	×	√
role inheritance	√	√	×	√	√	√
active access control	×	√	√	√	√	√
passive access control	√	√	×	√	√	√
separation of powers	√	√	√	√	√	√
dynamic authorization	×	√	√	√	√	√
Fine-grained access control	×	√	√	√	√	√

[16] Y. Song, Y. Peng and H. Ju, "OB4LAC: An organization-based access control model for e-government system," *Applied Mathematics Information Ences*, vol. 8, no. 3, pp. 1467–1474, 2014.

[17] R. K. Thomas, "Team-based access contural (TMAC): A primitive for applying role-based access controls in collaborative environments," in *International Conference on access control security*, pp. 13–19, Aug. 1997.

[18] Z. Thornton, T. H. Morris and I. Turnipseed, "Industrial control system simulation and data logging for intrusion detection system research," in *Annual Southeastern Cyber Security Summit*, pp. 1–14, June 2015.

[19] P. Wang and L. Y. Jiang, "Task-role-based access control model in smart health- care system," in *In MATEC Web of Conferences*, pp. 1–11, Mar. 2015.

[20] J. B. Xiong and Z. Q. Yaoand, J. F. Ma, "Behaviour-based multi-level access control for structured documents," *Journal of Computer Research and Development*, vol. 7, no. 4, pp. 53–62, 2013.

[21] H. Yang, A. Mohamed and M. Koien, "Access control model for cooperative healthcare environments: Modeling and verification," in *IEEE International Conference on Healthcare Informatics*, pp. 18–26, June 2016.

Biography

Dong Rui-hong biography. Vice researcher, worked at school of computer and communication in Lanzhou university of technology. His research interests include network and information security, information hiding and steganalysis analysis, computer network.

The Second Author biography. Xu Tongtong In 2017, Xu Tongtong obtained his bachelor of engineering degree from Xi'an University of Technology, he is studying for his masters degree at Lanzhou University of Technology. His research focuses on the industrial control network security.

The Last Author biography. It is required by the IJNS to have maResearcher/PhD supervisor, graduated from Gansu University of Technology in 1986, and then worked at school of computer and communication in Lanzhou University of Technology. He is vice dean of Gansu manufacturing information engineering research center, a CCF senior member, a member of IEEE and ACM. His research interests include network and information security, information hiding and steganalysis, multimedia communication technology.