Distributed Workflow Environment of the Adaptivity of Color Matching of Access Control Model

Xiaoxi Zhang
Institute of Disaster Prevention And Technology, Shijiazhuang, Hebei Province

Abstract: To in distributed workflow environment inIn order to make user get the most appropriate of permissions to implementation workflow taskOften need to user are assigned the role. For a group given authorization. of user best role Matching Problem Put forward a kind of distributed workflow environment of the adaptivity of Color Matching of access control model. The model can according to workflow of different task From System of role in looking for related task implementation permissions of a group or multi-role collection Then reference environment, Time Constraint and role between the inheritance relationship to the matching optimization Final for user select optimal of role collection. Experimental show that The model can eliminate redundant role For user accurate distribution a group the smallest role collection So as to achieve role matching optimization of objective.

Keywords: Access Control Distributed Workflow Role matching Environment and Time Constraint

1. Introduction

With the study of in-depth And has the many kinds of access control model. People from flexibility, Control Particle Size, Scalability and other aspects of traditional model the improvement Make its to active, Fine-grained, Different levels of orientation development And from task, Properties, Behavior and trust and new perspective to review the establishment of model[3]. King Serena and[9] Put forward the Based on Task-Role of access control (T-RBAC) Model will workflow decomposition into task Again will permissions by task distribution to role And permissions of distribution and task of context about Also has clear of role hierarchy Management, High scalability and adaptability[10] To achieve dynamic distribution management. King quiet yu and[11] Put forward of a kind of oriented cloud computing environment of property Access Control Model for at present complex information system of fine-grained access control and large scale user dynamic extension of Problem Through the Main Body, Object, Environment properties and permissions of Unified Modeling Describe authorization and access control constraints Make its has enough of flexibility and scalability. Li FengHua and[12] Put forward the based on behavior of access control security model given the behavior of concept and its management methods To solve Network Environment under support mobile Calculation of Information System of Access Control Problem. Sue talents such[13] Will MAC, the MAC (Mandatory Access Control) is often used security enhancing technique of operating system. Model and based on behavior of access control model Phase Combined Given Implementation Programme Solve access control process in user and data of classification management and problem. Lang Wave[14] Put forward of Oriented Distributed System Access Control of trust quantitative model for user division trust level According to the trust of Subjectivity, Fuzziness and uncertainty confidence-building Quantitative Model. Pay male and[15] The direct according to user of Real-Time Behavior Through corresponding algorithm calculation the
user of trust value and accordingly for user distribution Permissions.

In order to solve mixed role hierarchy structure in permissions Query, Role activation and role find and Problem Joshi Such.\[16\] Put forward only active set\(\text{set(Unique, Acti-vable)set UAS)}\) Of Concept Convenient the role hierarchy structure of analysis Simplified the role find of Process. For a given of a Group Permissions UASCAn in containing role inheritance and role activation relationship of hybrid role level in find out corresponding of only role collection But UASCCollection can't solve query optimal of role combination Problem. Willow and\[17\]OkayUASColl ect The Optimization Proposed minimum only role set\(\text{Minimi-zing uniquely roles MUR' MURAlgorithm according to user of access request to find role} \text{ln analysis different of access request of based on Get a group meet user request of role set. The algorithm in solving efficiency on the compared UASAAlgorithm But can't meet workflow environment in task-oriented request of security demand. ZhangSuch.\[18\] Defined. Based on RBAC Of user authorization query Problem User authorization query problemUAQ\[19\] Its using the greedy algorithm the search And use dynamic mutually exclusive role constraints Detection Once detection to don't meet the requirements of role combination to stop search Permissions request that was refused. Lu Such.\[19\]OkayUAQOf irreducible of and role collection permissions set of constraints this two aspects the Optimization Can effective match the character Can reduce the complexity of calculation and reduce operation time.

However more than access control model and can't completely meet distributed workflow environment in role of matching requirements. Because in distributed workflow environment in Task Permissions and role between the many-to-many of corresponding relationship more complex For user of access control permissions Often there are many kinds of role assignment programme This need to system will many group different of role collection assigned to user to achieve the same of authorized objective To.

Implementation System Task. This a diversification of authorized style will make system consumption a large number of calculation resources and storage resources to maintain these assigned relationship Need in System in looking for a group best role collection assigned to user To save system resources. But existing MUR The determine of minimum only role collection and does not take into account the distributed workflow of environment in permissions and role of more on dynamic mapping relationship The user in application last minute get of role collection not certain is only. This paper from role find this a issues Okay MUR The improved Put forward a kind of role matching of visit ask Control System Model 'Rolematching- rbac model RMT- RBAC\). According to the distributed environment different workflow of Task Type Use Role Lookup Algorithm And increase the role of matching conditions By different of environment and temporal Basis role between inheritance relationship of how much to looking for task implementation permissions of a group role set Finally will the role set accurate matching to user.

2. Based on Role matching of access control

In distributed workflow environment under User quantity increased Is set of role also complex changeable Especially in interaction process in There may be more than a role can complete the same confidential task. In for user group with match the character set of process in Combination of role quantity for at least the role set not certain is only. So Need to increase some role matching conditions Then to user matching just meet the demand of best role collection.

2.1 Put forward the access control model

In order to Implementation Task User Need To System Application Permissions And user and role, Role and permissions, Permissions and task is many-to-many of mapping relationship System can give user distribution and permissions relative should be of RoleTo by role to Implementation Task. Because the roles and permissions is many-to-many of the relationship So can by more a different of role to get with a Permissions. If other users have the permissions of other role The there may be security hidden danger. So This paper in and permissions corresponding of role set collection the
screening.Introduced a role matching mechanism to match the best role combination to distribution to user to improve safety.

Session setS: User and activation role between the Mapping. When user activation the part or all was granted the role when the establishment of the session. User implementation of permissions actually is in this session during activation of role Permissions.

Role matching RM: Every need to perform a task when find the set of roles that match the task from the set of roles in the corresponding autonomous domain. And assign Permissions. Also restrict permissions to roles that have inheritance to this collection.

Constraint Condition C: Rule
- constraints on various assignments in access control. Various assignment relationships are as follows:

2.2 Role matching

Permissions and users are associated. User gets permission by role assigned to it. Permission inheritance exists between roles, Enable a permission to be shared by multiple roles. A role may also have multiple Permissions, Therefore, certain permissions can be obtained through different role combinations. Therefore, In a distributed workflow environment, When a user requests one or more permissions to perform a task, There are often many different role assignment schemes.

To secure and secure access, Cannot assign redundant permissions to user, Need to find the best role combination and match it to the user. Considering the relationship between permissions and roles, Access can be obtained through different role combinations. Figure 2. A hierarchical tree of mixed roles for a system is given. Using Solid lines respectively, Dotted Line, Solid lines with arrows at both ends represent inheritance between roles, Activation Gate

Role collection discarded. Upper 3. Set of roles meet Mur Definition, All permissions that each role collection has (Include permissions for role inheritance) Not the same, But they can get permissions through partial inheritance of roles, Also the minimum role combination. The minimum role set matched by this kind of permission is not unique. So after you get multiple minimum set of roles, A valid role set matching mechanism is required (The mechanism must meet the minimum permission Principle, But also to ensure security) To match appropriate roles from and assign to the user.

Color Task, which the environment refers to implementation task of Platform (Hardware Platform, Software Platform and), Location (Place of physical location and network location and) And other and access control related of external objective information and Environment of collection Env Said. If role R Can in Environment Env Role role The can said Env(R) Env; Task which of temporal refers to in some time need to "with to related role to Implementation Task Time of collection Tim Said. If role R Can in temporal Tim Role role The can said Tim(R) Tim. This paper "with and security related of environment information and time information to constraint some role distribution Permissions To limit have these role of user access task of resources.

With R' Said by role lookup algorithm find the minimum role set With R'(I) Said R' In Elements. Different of role is available for different of environment and different of temporal. If in Environment Env And temporal Tim Situation under R'(I) Completely application environment and temporal requirements But R'(I) Only applicable temporal requirements The Selection

2.3 Role Matching Algorithm

Role Matching Algorithm of steps describe as follows:

Steps 1 Disconnect role hierarchy tree in all activation relationship Get a group independent of only with inheritance relationship of sub-tree;

Steps 2 For every tree only with inheritance relationship of sub-tree Looking for which don't contains permission inheritance relationship of role set. The character set any two role between all no permission inheritance relationship;

Steps 3 Will of earnings contains permission inheritance relationship of role set any
combination. All role combination of a collection;

Steps 4 According to complete task the need of Permissions, in previous step income of set collection select the most appropriate role combination of collection Au(R’);

Steps 5 According to task which of environment and temporal and role inheritance relationship of how much, Matching the best of role combination R’ And will the distribution to user.

This paper in MURA Algorithm of based on the improvement and expansion Reference literature

3. RMT-RBAC Implementation process

Step 1. User request access. User sends access request to server, Server checks user-sent identity information. If identity information matches, Allowed access; Otherwise refuse.

Step 2. Role matching. Depending on the task being performed, User gets different Permissions, RMT-RBAC Access Control Mechanism matches roles for users. First of all, Select the minimum set of roles for the corresponding permissions based on the role Lookup Algorithm, If the collection is unique, Then go to step 3; Otherwise, filter based on the environment and tense of the task, Filtered role collection if it is unique, Then go to step 3; Otherwise, filter based on the number of inheritance relationships in the role collection, Go to step 3.

Step 3. Access Authorization. Match the filtered roles to the user, User gets appropriate permissions for role. Step 4. Task execution. Users perform corresponding actions on tasks based on the permissions they have received.

4. Simulation Experiment

In this paper, the proposed role matching algorithm is simulated. MUR Algorithm comparison. Tu TU 2. The role hierarchy tree is shown for experimental comparison. In the experiment, the environment is set to work environment and public environment, Work time and work time, Different roles in different States, Specific as table 1. Listed.

Conclusion This paper proposed distributed workflow environment of the adaptivity of Color Matching of access control model. For implementation a task the need of a Group Permissions. In order to avoid role Redundancy Filter out the least number of roles in the set of roles to get the right to perform the task. But this set of roles may have multiple groups, So we added environmental constraints to the filtering process, Time Constraint and role inheritance, Then select the best set of roles from the above set of roles to match to the user, Remove additional set of roles by sifting. Optimized role Matching Problem. Filters to add roles will be considered in the future, Optimize the algorithm, To reduce algorithm complexity.

References


