J. Service Science & Management, **2009, 2: 107-116**
Published Online June 2009 in SciRes (www.SciRP.org/journal/jssm)

Access Control for Manufacturing Process in Networked Manufacturing Environment

Ke Zhou, Min Lv, Gang Wang, Bingyin Ren

Advanced Manufacturing Technology Center, School of Mechatronics Engineering, Harbin Institute of Technology, Harbin, 150001, China.
E-mail: k.zhou.hit@163.com

Received April 19th, 2008; revised September 16th, 2008; accepted November 10th, 2008.

ABSTRACT

The deficiencies of current access control techniques in solving the problems of manufacturing process access conflict in networked manufacturing environment were analyzed. An information model of manufacturing process was constructed, and a case XML Schema of manufacturing task model was given. Based on the characteristic analysis of the access control for the information model, an improved access control model of manufacturing process was constructed, and the access control model based on manufacture tasks, roles and time limits and the relationships among the elements were defined. The implementation mechanisms for access control model were analyzed, in which the access case matching strategy based on manufacture tasks and time limits, the authorization assignment mechanism based on manufacture tasks, roles, correlation degrees and time limits, XML based access control for transaction security and integrity were included. And the two-level detection architecture of transaction conflict was designed to find the conflicts both in application and in the database. Finally the prototype system was developed based on these principles. Feasibility and effectiveness of the method were verified by an enterprise application.

Keywords: *networked manufacturing, manufacturing process, access control, conflict resolution*

1. Introduction

Networked manufacturing is an advanced manufacturing mode. It is implemented by enterprises in order to response quickly to the market requirements and to promote the competition ability in the environment of knowledge economy and global manufacturing [1]. Access control is one of the most pervasive security mechanisms in use today [2]. It concerns whether specific users or processors can access specific system resources or not and which operation types they are allowed.

Many issues in access control are studied in order to implement information interaction in multi-user system. Some control models are put forward, such as Access Control Lists (ACLs) [3], Access Control Matrixes (ACM) [4], Discretionary Access Control (DAC) model [3], Role-Based Access Control (RBAC) model [5], Task-Based Access Control (TBAC) model [6], Task-Role-Based Access Control (TRBAC) model [4]. Although these models have been widely discussed and applied in various fields [7−10], detailed discussion is needed in order to provide an effective access control mechanism for manufacturing process in networked manufacturing environment.

Present access control strategies applied in networked manufacturing were focused on access issues for public information, such as resource information, process planning information, design information, product data information, etc. The access control for manufacturing process has not been studied intensively yet. There are two reasons for it. One is that there are too much data about manufacturing process, and many of them are very hard to be collected because of the old machine tools. The other one is that the access to manufacturing process is much more flexible because of the multitudinous constraints between users and access objects, after manufacturing process is split and manufacturing tasks are merged in networked manufacturing environment. That makes the access control more difficult. Real-time manufacturing process supervision becomes more executable as the technology of digital supervision, remote control and network is developed. Data of manufacturing process would be quite open to numerous users in networked manufacturing environment. That means effective access control is completely necessary to protect manufacturing process data and ensure the fluent execution of networked manufacturing.

The eXtensible Markup Language (XML) [11] has emerged as the defacto standard for storing and exchanging information in the Internet Age. Several attempts are being made to ensure security over the Internet, especially for web services, including confidentiality, integrity, authentication, authorization, key management and security enforcement mechanism. Row-level security (RLS) feature provides fine-grained access control (FGAC) which means the control is at the individual row level. Virtual private databases (VPD) security provides a whole new way to control access to Oracle data.

In this paper, based on the characteristic analysis of the access control for manufacturing process in networked manufacturing environment, an access control model of manufacturing process was constructed, and the access control model based on manufacture tasks, roles and time limits and the relationships among the elements were defined. The implementation mechanisms for access control model were analyzed, in which the access case matching strategy based on manufacture tasks and time limits, the authorization assignment mechanism based on manufacture tasks, roles and time limits, the resolution mechanism of concurrent operation conflicts were included. Then the problem of manufacturing process access among allied enterprises was solved.

2. Related Work

ACLs and ACM [3,4] is earlier access control model. The two models are simple and intuitive. But the disadvantage is that they can't deal with large amount of data. When the number of subjects and objects becomes huge, the cost of managing ACLs or ACM multiplies. Therefore, they are not suitable for large enterprises. In DAC model [3], the owner of computer resources or anyone authorized decide who can access these resources. Among the above methods, the subjects they face are only single user. And the security administration and review is very complicated [3]. The concept of RBAC began with multi-user and multi-application on-line systems pioneered in 1970s [12]. The central motion of RBAC is that permissions are associated with roles, and users are assigned to appropriate roles. Roles are created for the various job functions in an organization and roles are assigned to the users according to their responsibilities and qualifications. In RBAC, roles can be easily reassigned from one user to another, which greatly simplifies the management of permissions. But the method doesn't support the active access control in workflow environment. TBAC [6] considers workflow as a set of tasks that are linked to achieve a common goal. The model dynamically manages the permissions through the tasks and tasks' states. It distinguishes the access right assignment and access right activation. And it supports dynamic activation of access right needed in workflow systems. But it is difficult to combine with roles. T-RBAC [4] is based on RBAC model, and therefore it contains the basic features of RBAC. However, it is more than RBAC. It analyzes the types of task in enterprise organization, and connects the users with permission through role and task. It supports task level access control, both active and passive access control, different access control strategy according to task class, and partial inheritance of access rights in the role hierarchy. However, it doesn't support the object hierarchy and operation hierarchy. The TRBAC model in paper [13] can meet the need to manage and enforce the strong and efficient access control technology in large-scale Web environments. The implementation of TRBAC on the Web is also illustrated. Finally, the Web application adopting the TRBAC model, called E-Government Official Document Flow & Processing System, is given to demonstrate the feasibility.

EXtensible Markup Language (XML) specification [14] is the work of the World Wide Web Consortium (W3C) Standard Generalized Markup Language (SGML) Working Group. It is designed as a meta-language for Internet use. Its objectives are to overcome the rigid HyperText Markup Language (HTML) tagging scheme while providing Web users with a means for defining their own domain specific tags and attributes. XML is used in the integration of applications which makes data sharing and communication within applications easier and uniform. Security is an important aspect of web services. Securing XML data is critical to the success of any web based applications or web services. Some practical concepts that can be employed in an enterprise environment for managing security policies using XML are described. An example is given using the proposed concepts with Java and Role-Based Access Control (RBAC) policies [15]. In paper [16], the context-aware access control architecture is present in order to support fine-grained authorizations for the provision of e-services, based on an end-to-end web services infrastructure. Access permissions to distributed web services are controlled through an intermediary server, in a completely transparent way to both clients and protected resources. The access control mechanism is based on RBAC model, which incorporates dynamic context information, in the form of context constraints. Context is dynamically updated and provides a high level of abstraction of the physical environment by using the concepts of simple and composite context conditions. In paper [17], they focus on XML-based access control languages and, in particular, on the eXtensible Access Control Markup Language (XACML), a recent OASIS standardization effort. XACML is designed to express authorization policies in XML against objects that are themselves identified in XML. XACML can represent the functionalities of most policy representation mechanisms.

Row-level security (RLS) feature is introduced in Oracle8i. It provides fine-grained access control (FGAC) which means the control is at the individual row level. Virtual private databases (VPD) security provides a whole new way to control access to Oracle data. Most interesting is the dynamic nature of a VPD. At runtime, Oracle performs these near magical feats by dynamically modifying the SQL statement of the end user [18]. Rather than opening up an entire table to any individual user who has any privileges on the table, row-level security restricts access to specific rows in a table. The result is that any individual user sees a completely different set of data, only the data that person is authorized to see. In paper [19], the limitations and shortcomings of security design of the traditional database access control model are analyzed. Projects of VPD design based on role access control are presented [19,20]. The question of the inconsistency of users' authority management for application system and database management system in ORACLE DB brings insecurity to database. RBAC technology is used to implement users' authority control for front and back system in paper [21].

3. Manufacturing Process in Networked Manufacturing Environment

3.1 Access Control for Manufacturing Process in Networked Manufacturing Environment

Manufacturing process of product is composed of a series of manufacturing tasks according to production flow in discrete manufacturing industry [22]. In networked manufacturing environment based on ASP, manufacturing process is split to a series of tasks after requirements are committed to Application Service Provider (ASP) by manufacturing requirement enterprises. Then manufacturing tasks are merged and distributed to execution enterprises. Therefore access to manufacturing process should be split into access to tasks and reorganized.

Real-time data of manufacturing process were transferred through network from manufacturing fields to manufacturing execution enterprises and manufacturing requirement enterprises to monitor the process and communicate. There are several characteristics in access control for manufacturing process in networked manufacturing environment.

1) Distribution of user privilege was constrained dynamically by manufacturing process. Access privilege distributed to user was not invariable, but varied with the change of manufacturing tasks. Following with the manufacturing process, access privilege of various roles would be changed with the flowing of workflow. And operations of access object were given different priorities.

2) User privileges were interdependent and mutually-restrained. Manufacturing information was shared by users in networked manufacturing through network to increase the resource utilization rate. Access to some information was limited of the number of visits. For example the application of the simulation software would be limited of point number purchased. It is the key of access control for manufacturing process that how to distribute the authority to the users to maximize the efficiency of limited resources.

3) Distribution of user privileges was constrained by time limits. High-quality product and delivery on schedule is the basis of long-term collaboration of enterprise. Adjusting of users' privileges was necessary based on time limits besides assigning authorization based on manufacturing tasks.

3.2 Information Model of Manufacturing Process

Manufacturing information flow in networked manufacturing environment was studied to make the manufacturing information model more reasonable. Products and process planning were designed by design department after the enterprise received orders. Then production was organized by production department according to process planning design information. Products were manufactured according to resource utilization information and production plan/schedule. Resource configurations were optimized by dispatching department according to the equipment utilization rates, site utilization rates and so on. Quality information was collected into the financial department after the products were manufactured. The quality-cost analysis information was put forward by the financial department which could be an index to optimize the designs, production planning and manufacturing processes. Every department could be in different places in networked manufacturing environment. Therefore the manufacturing information interaction was more difficult. A manufacturing information model was constructed to describe information interaction of design, manufacturing, quality inspection and resource utilization among allied enterprises.

As the object of access control, manufacturing processes information mainly includes information of manufacturing tasks, dispatching, quality of on line products, product quality inspection, machine tools, fixture tools, work-piece rough, product structure information and NC programs. Manufacturing tasks and dispatching organizes production by the ID of product resources (example as machine tool, fixture tool). Machining accuracy, economic parameter and utilization efficiency influences task allocation and dispatching making. Quality information of on line products, product quality inspection information and quality statistics information use manufacturing task information to trace and compute product

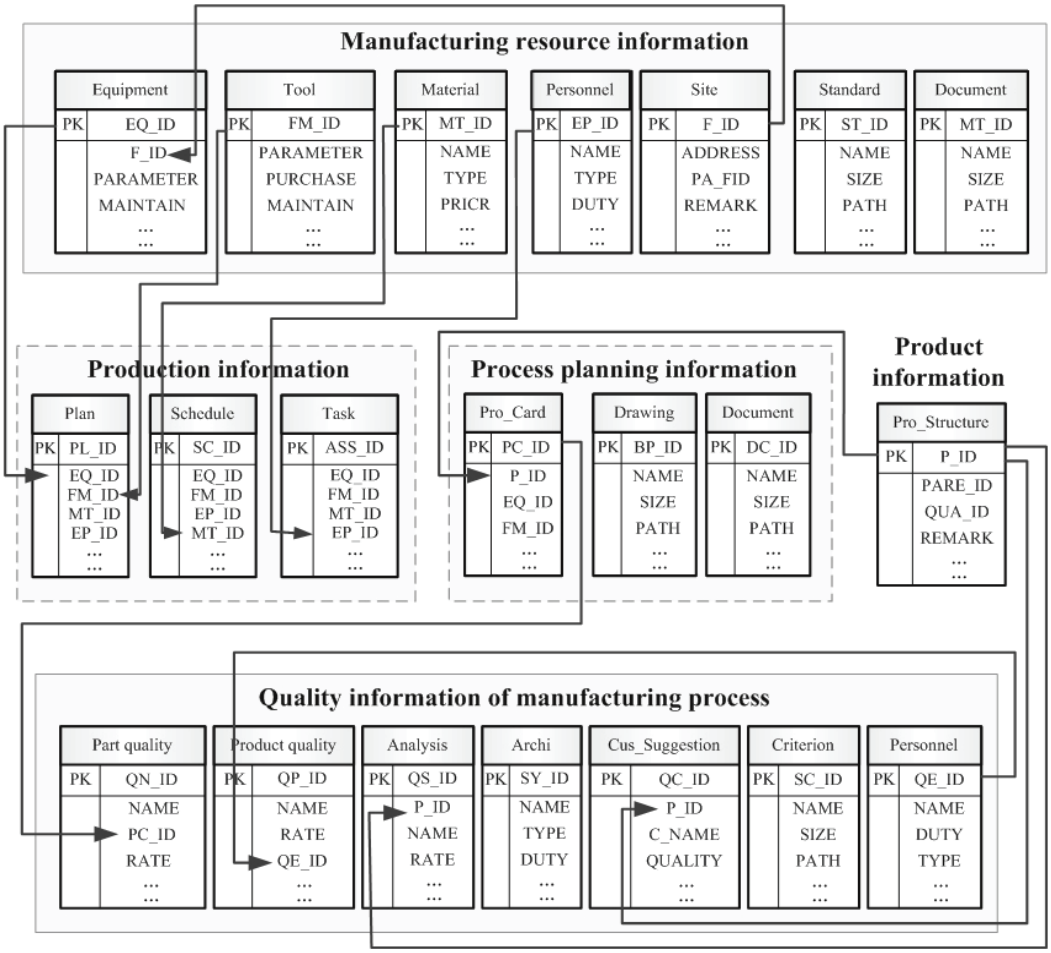

Figure 1. Partial information model of manufacturing process

```
<xsd : element name="MT">
    <xsd : complexType>
        <xsd : element name="Input" minOccurs="0"/>
        <xsd : element name="Output" minOccurs="0"/>
        <xsd : element name="Deadline"/>
        <xsd : element name="Status"/>
        <xsd : element name="Description "/>
    <xsd : attribute name="Id" type="xsd : NMTOKEN" use="required"/>
    <xsd : attribute name="Name" type="xsd : string"/>
    </xsd : complexType>
</xsd : element>
<xsd : element name="MT">
    <xsd : complexType>
        <xsd : element name="MT"
        minOccurs="0" maxOccurs="unbounded"/>
    </xsd : complexType>
</xsd : element>
<xsd : element name="Deadline" type="xsd : string"/>
<xsd : element name="Status" type="xsd : string"/>
<xsd : element name="Description" type="xsd : string"/>
```

Figure 2. The case XML Schema of manufacturing task model

quality. Meanwhile, feedback information of quality has influence on task dispatching. Partial information model of manufacturing process was showed in Figure 1. The case XML Schema of manufacturing task model is showed in Figure 2.

4. Access Control Model of Manufacturing Process

Objects and operations of access were controlled by users' roles in traditional Role-Based Access Control (RBAC) model. But there are other factors influencing access authorization in networked manufacturing environment, such as manufacture tasks, correlation degrees, time limits. Based on the characteristic of access control for manufacturing process, an improved access control model based on manufacture tasks, roles and time limits was constructed as showed in Figure 3. The elements and the relationships among the elements were defined as below.

Definition1. The access control model based on manufacture tasks, roles and time limits was a eleven-dimension array $\langle MT, R, U, Tl, W, S, O, OP, C, P, SP\rangle$, where:

Manufacture task sets (*MT*): the tasks in the manufacturing system. Task was a basic unit to accomplish one working target. There were five states in the task lifecycle: initial state, active state, suspensive state, terminative state and revocatory state. They were quantized respectively as 30, 40, 20, 10 and 0.

Role sets (*R*): A role was a group of interrelated authorizations. Usually one role delegated one work or position in an organization or a task. Roles could be administrative positions or technical roles in a manufacturing system.

User sets (*U*): the independent subjects that could access the information in the system.

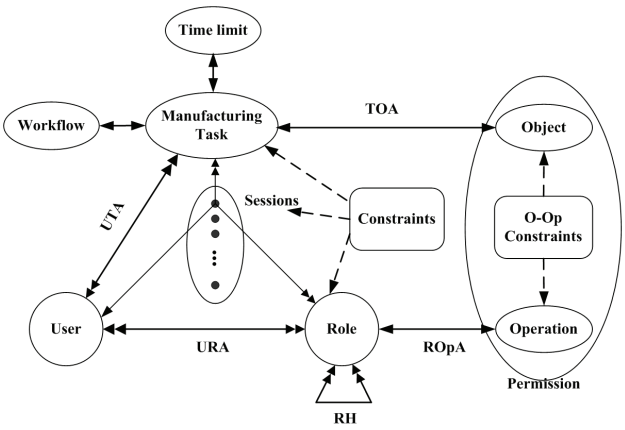

Figure 3. Improved access control model based on manufacture tasks, roles and time limits

Workflow sets (*W*): Manufacture tasks (*MT*) were split into subtasks and activities as workflows.

Time limit state sets (*Tl*): Let the time limit of a certain manufacture task be *th*, and the past time of the task be *tp*. Then the time limit state of the task was calculated by formula: $tl = 100 \times (tp - th) / th$.

Session sets (*S*): the corresponding relations of users, roles and tasks.

Object sets (*O*): the objects that were accessed and controlled.

Operation sets (*OP*): the minimum actions that accomplished some function to the controlled objects such as a query of data. The sets of operations which would not influence databases were recorded as OPN. And the sets of operations which would influence databases were recorded as OPE. $OP = OPN \bigcup OPE$, $OPN \bigcap OPE = \varnothing$.

Constraint sets (*C*): a series of constraint conditions in which constraints of task-role assignments, constraints of object-operation assignments and other constraints were included.

Permission sets (*P*): the sets of authorized operations to objects. $P \subset Op \times O$.

Security Policy sets (*SP*): the sets of security policies of users.

Definition2. MT-object assignments (*MTOA*): the corresponding relationship of manufacture tasks and objects. $MTOA \subset MT \times O$.

Definition3. User-MT assignments (*UMTA*): the corresponding relationship of users and manufacture tasks. $UMTA \subset U \times MT$.

Definition4. User-role assignments (*URA*): the corresponding relationship of users and roles. $URA \subset U \times R$.

Definition5. Role-operation assignments (*ROpA*): the corresponding relationship of roles and operations. $ROpA \subset R \times Op$.

Definition6. Hierarchical relations of roles (*RH*): the relations of roles' hierarchy which were showed in Figure 4. $RH \subset R \times R$.

Definition7. MT-workflow assignments (*MTW*): the corresponding relationship of manufacture tasks and workflows. $MTW \subset MT \times W$.

The access control model based on manufacture tasks, roles and time limits was constructed in definition 1. Some elements (such as *MT*, *Tl*, etc.) were extended on the basis of traditional RBAC. Therefore access authorization assignment would be adjusted based on manufacture tasks, roles, correlation degrees and time limits, when conflicts appeared. And matching operations to

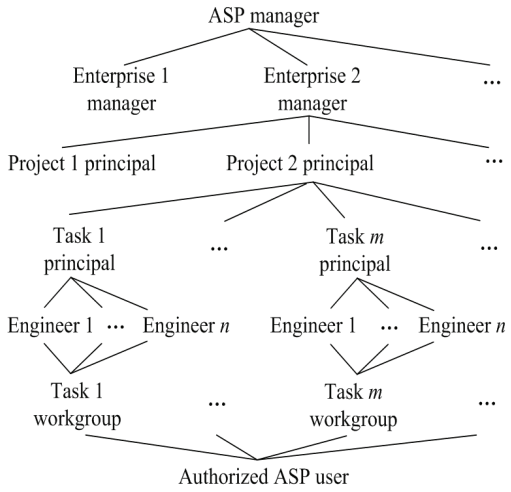

Figure 4. Hierarchy of roles

objects were reduced because of the relationship of objects, tasks, users and their roles. Then the efficiency of access control was increased.

5. Implementation Mechanisms for Access Control Model

As it described in Figure 5, access to manufacturing process would be controlled by following the steps as below after users log in the system.

Step 1: Get user's operation right ropa, corresponding security policy sp, authorized access object and task state tl according to definitions from 1 to 5 after task state and role of the user is identified automatically by the system.

Step 2: Start access matching mechanism based on manufacturing tasks, role and time limit to compute case similarity S.

Step 3: Compare maximum of case similarity (Max S) with ideal matching factor S_0. Users' permission would be obtained by reusing the corresponding access case if Max $S \geq S_0$. Compute users' priorities p by implementing authorization assignment mechanism based on manufacture tasks, roles and time limits if Max $S < S_0$.

Step 4: Generate access interface or windows with object lists, operation menus and function buttons according to p.

Step 5: Requirement for user's operation is sent from client to server, such as process checking, task editing, software calling and so on.

Step 6: Judge whether software/document is needed or not. Go to step 7 if it is, else go to step 11.

Step 7: Judge whether calling overruns the limit or not if it needs to call software. Judge whether the file is being edited or not if it needs to call document. The XML based access control for transaction security and integrity would be started if it is. Go to step 8 if it is not.

Step 8: Operations on objects are executed by users.

Step 9: Both access object and operation right of the user was released after the operation was sent from client to server.

Step 10: Go to step 4 if other objects will be visited. Exit the system if all operations are completed.

Step 11: Judge if user's operations need to edit data in database. Go to step 12 if it does. Go to step 8 if it does not.

Step 12: The XML based access control for transaction security and integrity will be started if the data are being edited. Go to step 8 if they are not.

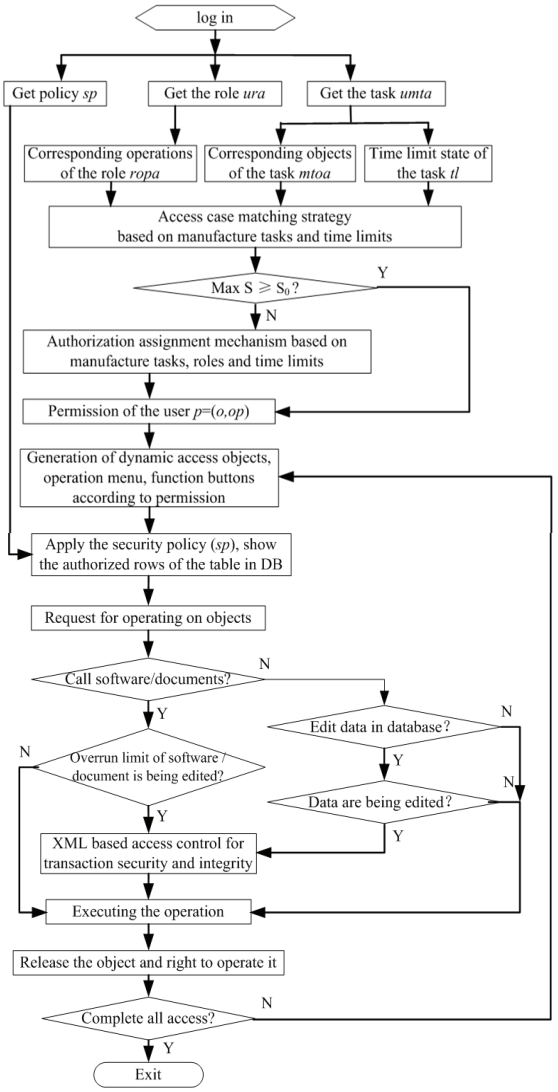

Figure 5. Access control for manufacturing process in networked manufacturing environment

5.1 Access Case Matching Strategy Based on Manufacture Tasks and Time Limits

Splitting of manufacturing process and merging of manufacturing tasks becomes more complicated as users increase in networked manufacturing platform. Then the calculation of access assignment is increasing with geometric series. That makes the efficiency of access control decrease. According to the characteristics of sufficient access cases and high reusability, the access case matching strategy based on manufacture tasks and time limits was implemented in order to assign access authorization quickly and increase the efficiency of access control for manufacturing process.

History of authorization assignments and access control cases was saved in databases as instance to provide references for next assignment. Weighted retrieval algorithmic based on similarity was adopted to search useful instances more rapidly and exactly.

Characteristic expression of access cases A was $A(C_i)$. The format of C_i (characteristic sets) was $\{C_1, C_2,\ldots, C_n\}$, $C_i (1 \le i \le n)$ meant a certain characteristic, such as role type, time limit state, task state, etc. Every characteristic had two parameters, characteristic value (p_i) and weight value (q_i). Suppose there were two access cases P_1 and P_2, their characteristic expression were $A_1(C_{i1})$ and $A_2(C_{i2})$ $(1 \le i \le n)$. Then the calculation formula of the dissimilarity $D(A_1, A_2)$ was as below.

$$D(A_1,A_2)=\sum_{i=1}^{n}\left|\frac{q_{i1}}{\sum_{i=1}^{n} q_{i1}} p_{i1}-\frac{q_{i2}}{\sum_{i=1}^{n} q_{i2}} p_{i2}\right|$$

Then the calculation formula of the similarity $S(A_1, A_2)$ was as below.

$$S(A_1,A_2)=1-D(A_1,A_2)=1-\sum_{i=1}^{n}\left|\frac{q_{i1}}{\sum_{i=1}^{n} q_{i1}} p_{i1}-\frac{q_{i2}}{\sum_{i=1}^{n} q_{i2}} p_{i2}\right|$$

Then, $0 \le S(A_1,A_2) \le 1$.

Users' permission would be obtained by reusing the corresponding access case if Max $S \ge S_0$. Users' priorities p would be computed by implementing authorization assignment mechanism based on manufacture tasks, roles and time limits if Max $S < S_0$.

5.2 Authorization Assignment Mechanism Based on Manufacture Tasks, Roles and Time Limits

Authorization assignment mechanism based on manufacture tasks, roles and time limits would be started when similarity degrees between new case and each of the cases in the database did not satisfy ASP manager which meant Max $S < S_0$. The rules listed below were followed in the authorization assignment.

Rule1. Permission was computed by p=(o,op) according to definition 1 – 5. And it was composed of access objects (o) and corresponding operations (op). Where, access object (o) was obtained by the task which was executed by the user (*umta*) and MT-object assignments (*mtoa*), and corresponding operation (op) was obtained by the role of user (*ur*a) and role-operation assignments (*ropa*).

Rule2. Operations which would not influence databases were opened to all the authorized users.

Rule3. The edit authorization was assigned to one user in one task in the same time.

Rule4. The edit authorization was assigned to the task first which was in the active state, when the same data was called by different tasks.

Rule5. The edit authorization was assigned to the task first which was in the exigent state, when the same data was called by different tasks which were all in the active state.

Rule6. The edit authorization would be canceled and assigned to the next user whose task was in the active state automatically when tasks, roles, or the roles to execute the task overran the limit of time.

Rule7. A user would be allowed to delete only if all correlative tasks were in the terminative state or revocatory state.

Rule8. A role would be allowed to delete only if the correlative user set was empty.

5.3 XML Based Access Control for Transaction Security and Integrity

5.3.1 Two-Level Detection Architecture of Transaction Conflict

XML based access control for transaction security and integrity is based on the transaction conflict detection. We designed a kind of two-level detection architecture of transaction conflict to find the conflicts both in application and in the database. The detection architecture is showed in Figure 6.

The application or data would be locked when a conflict is detected in order to assure the security and integrity of transaction. Resolution mechanism of access conflicts would be started when the access sequence should be adjusted. The mechanism was based on role's type, correlation degree, manufacture task state and its time

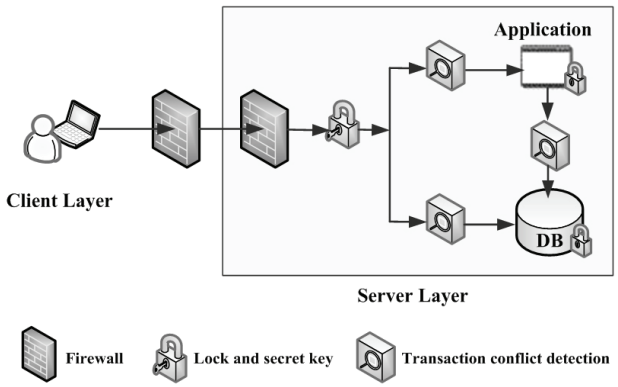

Figure 6. Two-level detection architecture of transaction conflict

limit in order to coordinate operations of users and resolve the access conflicts. The core of the mechanism was how to evaluate users' priorities, and how to adjust their authorities according to the priority sequence. Suppose there the users in some access to manufacturing process were U={u_1, u_2,…, u_n}, then the factor aggregate which will influence the priority of access degree was X={x_1, x_2, x_3, x_4}={ types of access, related degree of access object, task state, time limit state }. Quantization of priority factors, calculation of priority factor and steps of conflict resolution were included in the resolution mechanism.

5.3.2 XML-Based Security Standards

Several attempts are being made to ensure security over the Internet, especially for Web services. These approaches are XML-based, message-level security solutions, and can also be used for manufacturing process services based on Web services.

Confidentiality. When a sender transmits XBRL and XARL documents to a recipient through the Internet, the documents remain confidential. That is, only the sender and intended recipient can read the message.

Integrity. When a sender transmits XBRL and XARL documents to a recipient through the Internet, the documents have not been changed. In other words, XBRL and XARL documents received by the intended recipient are exactly the same as the documents transmitted by the sender.

Authentication. When XBRL and XARL documents are received by a user or system, the sender and receiver are who they claim to be. Non-repudiation When XBRL and XARL documents are sent to a receiver, the sender cannot later deny having sent the documents, and vice versa, the recipient cannot deny having received the documents.

Authorization (Access control). Only authorized users are able to access the XBRL and XARL documents.

Key management. Encryption is used to maintain confidentiality of information transmitted over the Internet. Encryption involves the use of private and/or public cryptographic "keys" to encipher transmissions. It is important to ensure proper creation, storage, use, and destruction of each cryptographic key. Audit trails are also needed to trace user accesses and actions. They also can be used to ensure system integrity through verification.

Security enforcement mechanism. Financial service providers can define a security policy with varying privileges and enforce it across various platforms. Audit trails Audits trails are a series of records of system events such as user accesses and user activities. Audit trails can enhance user accountability by tracing the user's activities, to reconstruct system events after a problem has occurred, to monitor problems, and to detect system intrusion.

6. Application of the System and Analysis of Cases

A prototype system of access control for manufacturing process in networked manufacturing environment was developed based on principles above. And it was applied in a steam turbine factory. Distributed computing architecture, Browser/ Server mode and J2EE structure criterion were adopted in this system considering some factors in networked manufacturing environment such as region and security. There were four layers in this system, client layer, interface expression layer, business logic layer and data service layer. The interface of messaging suspended operation to users was showed in Figure 7.

7. Conclusions

The proposed access control model of manufacturing process in networked manufacturing environment and the implementation mechanisms were applied in developing the access control system. The system was verified by the application in a networked collaborative design and manufacture platform of steam turbine factory. The results showed that the access conflicts were resolved by the implementation of mechanisms for the access control model, in which the access case matching strategy based on manufacture tasks and time limits, the authorization assignment mechanism based on manufacture tasks, roles, correlation degrees and time limits, XML based access control for transaction security and integrity were included. The results also indicated that by using the method the users' operations in the allied enterprises were coordinated, the resource configuration conflicts were reduced, and the resource utilization rate was increased. At the same time the efficiency of access control for manufacturing process was increased, and the manufacturing cycle time was shortened.

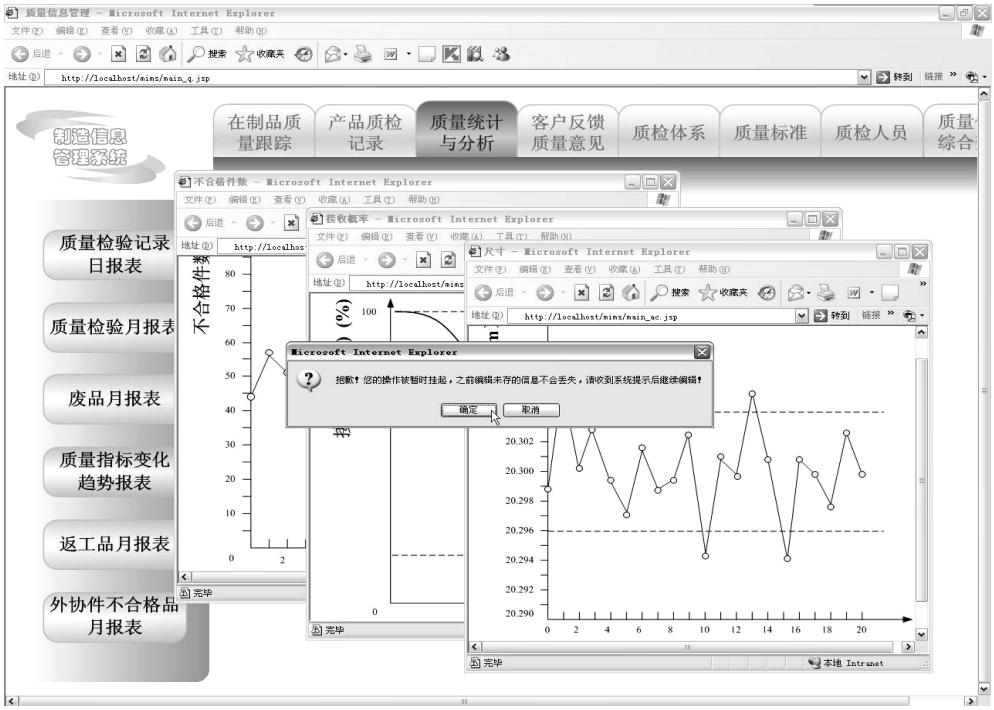

Figure 7. Interface of messaging suspended operation to users

REFERENCES

[1] Y. S. Fan, "Connotation and key technologies of networked manufacturing," Computer Integrated Manufacturing Systems, Vol. 9, No. 7, pp. 576−582, 2003.

[2] P. Ward and C. L. Smith, "The development of access control policies for information technology systems," Computers & Security, Vol. 21, No. 4, pp. 356−371, 2002.

[3] C. P. Pfleger, "Security in computing," 2nd Edition, Prentice-Hall International Inc., Englewood Cliffs, NJ, 1997.

[4] S. Oh and S. Park, "Task-role-based access control model," Information Systems, Vol. 28, pp. 533−562, 2003.

[5] J. Hwang, K. Wu, and D. Liu, "Access control with role attribute certificates," Computer Standards & Interfaces, Vol. 22, pp. 43−53, 2000.

[6] J. Deng and F. Hong, "Task-based access control model," Journal of Software, Vol. 14, No. 1, pp. 76−82, 2003.

[7] T. Xin and I. Ray, "A lattice-based approach for updating access control policies in real-time," Information Systems, Vol. 32, pp. 755−772, 2007.

[8] S. Fu and C. Z. Xu, "Coordinated access control with temporal and spatial constraints on mobile execution in coalition environments," Future Generation Computer Systems, Vol. 23, pp. 804−815, 2007.

[9] H. X. Cai, T. Yu, and M. L. Fang, "Access control of manufacturing grid," Computer Integrated Manufacturing Systems, Vol. 13, No. 4, pp. 716−720, 2007.

[10] C. Liang, T. Y. Xiao, L. X. Zhang, "Access control for collaborative environment in networked manufacturing system," Computer Integrated Manufacturing Systems, Vol. 13, No. 1, pp. 136−140, 152, 2007.

[11] T. Bray, J. Paoli, and C. M. Sperberg-McQueen (Eds), "Extensible Markup Language (XML) 1.0 (2nd Ed.)," W3C Recommendation, October 2000.

[12] R. Sandhu, E. J. Conyne, H. Lfeinstein, and C. E. Youman, "Role based access control models," IEEE computer, Vol. 29, No. 2, pp. 38−47, 1996.

[13] W. H. Chen, X. C. Yin, B. Mao, and L. Xie, "A task and role-based access control model for web," Journal of Computer Research and Development, Vol. 41, No. 9, pp. 1466−1473, 2004.

[14] Extensible Markup Language (XML) 1.0-W3C Recommendation 10-Feb-98.

Http://www.w3.org/TR/1998/REC-xml-19980210.

[15] N. N. Vuong, G. S. Smith, and Y. Deng, "Managing security policies in a distributed environment using eXtensible Markup Language (XML) ," SAC, pp. 405−411, 2001.

[16] V. Kapsalis, L. Hadellis, D. Karelis, and S. Koubias, "A dynamic context-aware access control architecture for e-services," Computers & Security, Vol. 25, pp. 507−521, 2006.

[17] C. A. Ardagna, E. Damiani, S. De Capitani di Vimercati, and P. Samarati, "XML-based access control languages," Information Security Technical Report. Vol. 9, No. 3, pp. 1363−4127, 2004.

[18] C. Lu, X. J. Hu, C. L. He, etc., "Oracle 10g DBA," Publishing House of Electronics Industry, January 2007.

[19] L. Y. Wan, "Project of a VPD design based on role access control in Oracle," Journal of Jiangxi Institute of Education (Comprehensive), Vol. 28, No. 3, pp. 33−36. 2007.

[20] L. Yao, and H. Z. Chen, "Oracle HTML DB application with virtual private database," System Simulation Technology, Vol. 2, No. 4, pp. 244−248, 2006.

[21] A. L. Zhong and F. H. Xu, "A method of using management of role to enhance the security of ORACLE database," Journal of Chengdu University (Natural Science Edition), Vol. 26, No. 3, pp. 225−227, 2007.

[22] K. Zhou, X. X. Wen, G. Wang, M. Lv, and Y. Q. Gong, "Key technologies of manufacturing information system management supporting networked manufacturing," IEEE International Conference on Engineering, Services and Knowledge Management (the Management track of WiCom 2007), Shanghai, China, pp.6240−6243, September 23−25, 2007.

