# TCBAC: An Access Control Model for Remote Calibration System

Zhuokui Wu
School of Mechanical & Automotive Engineering, South China University of Technology, Guangzhou, China
College of Automation, Zhongkai University of Agriculture and Engineering, Guangzhou, China
Email: wuzhuokui@126.com

Guixiong Liu
School of Mechanical & Automotive Engineering, South China University of Technology, Guangzhou, China
Email: megxliu@scut.edu.cn

***Abstract*—In order to improve the reliability of remote calibration system, a task-constraint-based access control model named TCBAC is presented according to the characteristic of remote calibration system. TCBAC conducts access control according to task. It defines authorization constraints and execution constraints by the characteristics of task and the relation among tasks. Users can obtain a task authorization only when the authorization constraint is satisfied, and can execute a task only when the execution constraint is satisfied. The performance of TCBAC is analyzed by applying it to a remote calibration system and comparing it with DAC, MAC and RBAC which are commonly used access control models at present. The results show that TCBAC has the advantages of considering context and dynamics, it more fully satisfies the principle of least privilege and the principle of separation of duty and has good expansibility.**

***Index Terms*—access control, remote calibration, metrology, instrument, task**

## I. Introduction

Calibration is a kind of behavior which ensures the normal operation of measuring instrument [1]. It concerns industrial and agricultural production, national defense construction, scientific experiments, domestic and foreign trade and the health and safety of the people. With the development of measurement, computer and network technologies, remote calibration technology rises gradually and has become a research hotspot [2]. Remote calibration technology strongly extends measurement assurance program, greatly shortens calibration time, and realizes the high efficiency and low cost of calibration work.

Some kinds of remote calibration system have been presented at present, such as remote calibration system of resistor [3][4], remote calibration system of pressure sensor [5], remote calibration system of temperature sensor [6], general remote calibration platform based on Internet [7], etc. These remote calibration systems solve the technical problems of realizing remote calibration operation, but don't fully consider the reliable problems of remote calibration operation. Reliability directly affects the practicability, popularization and application of remote calibration system. It's a key problem must be solved in the development of remote calibration system.

Access control technology is used to divide the permission of operator and prevent from abusing permission. It ensures calibration operation can be completed safely and reliably. It's an important part of reliable technology for remote calibration system. Traditional access control technology mainly includes DAC, MAC and RBAC at present [8][9][10]. But remote calibration system is a kind of multiple task system which is used to complete calibration operation and related auxiliary operation, these traditional access control technologies can't closely connect with the task operation of remote calibration system because of their static authorization mechanism, then the fine granularity access control can't be conducted and some safety problems are caused. So it's very important to build the dynamic access control mechanism which can closely connect with the task of remote calibration system and conduct fine granularity access control according to calibration task.

Aiming at these problems, a task-constraint-based access control model named TCBAC for remote calibration system is presented. TCBAC closely connects with the task of remote calibration system, conducts fine granularity access control according to calibration task and considers the dynamic change of task. So it has good safety and can improve the reliability of remote calibration system.

## II. Basic Structure and Access Control Analysis of Remote Calibration System

### A. Basic Structure

The basic structure of remote calibration system is shown in Fig. 1. The calibration method by the structure is described as follows: The user of metrology institution carries out the operations of sending command and receiving result through the Internet, and the user of calibration site carries out corresponding operations by receiving control commands and feeds back results to the user of metrology institution.


doi:10.4304/jsw.8.12.3139-3145

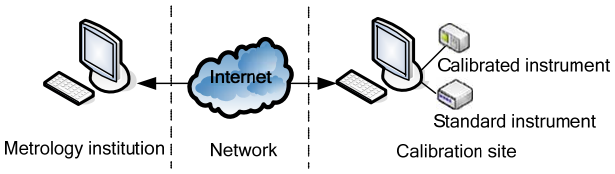


Figure 1. The basic structure of remote calibration system

### B. Access Control Analysis

Remote calibration system has the characteristic of multiple tasks. The main tasks of remote calibration system include information registration, information audit, instrument information management, calibration application management, calibration process management and calibration result management, etc. Some large tasks also contain multiple child tasks.

The access control mechanism of remote calibration system is very important to the reliability of calibration operation in open network environment. For the remote calibration system which has the characteristic of multiple tasks, the access control mechanism needs to guarantee that a user can do which tasks and can't do which tasks and every task operation has a corresponding user, achieves the traceability of the running of remote calibration system, then improves the reliability of remote calibration system. So it needs to build a dynamic access control model based on task. The model needs to meet the following requirements:

(1) The principle of least privilege. The principle of least privilege means that the permissions which a user has can't exceed the permissions which the user uses to execute the task. In a remote calibration system, it means restricting the permission of a user extremely to ensure the safety of remote calibration system under the precondition that calibration task can be completed successfully.

(2) The principle of separation of duty. The principle of separation of duty means achieving the goal of supervising each other by assigning tasks reasonably. In remote calibration system, the first use of the principle is to ensure the correctness of remote calibration operation , the second use of it is to ensure no users can't do fraudulent activities in the system, so the reliability of remote calibration system is improved.

## III. TASK-CONSTRAINT-BASED ACCESS CONTROL MODEL NAMED TCBAC

The TCBAC model is described in detail from task, task-constraint-based access control and TCBAC model below.

### A. Task

Task is the access unit of TCBAC. Task is defined as Definition 1 from the access control perspective.

**Definition 1.** Task: It means a specific work assigned to a user. It includes multiple permissive operations to multiple objects from the access control perspective. All the tasks of a system are expressed as a set of $TASK = \{task_i | i = 1,2,3,...\}$.

If all the operation permissions of a system are expressed as a set of $PERM = \{perm_i | i = 1,2,3,...\}$ and all the objects of a system are expressed as a set of $OBJ = \{obj_i | i = 1,2,3,...\}$, then an instance of task named $task_1$ can be shown as Fig. 2. The $task_1$ contains some operation permissions to three objects named $obj_1$, $obj_2$ and $obj_3$ which are the operation permissions named $perm_1$, $perm_2$ and $perm_3$ to $obj_1$, the operation permission named $perm_1$ to $obj_2$ and the operation permission named $perm_2$ to $obj_3$.

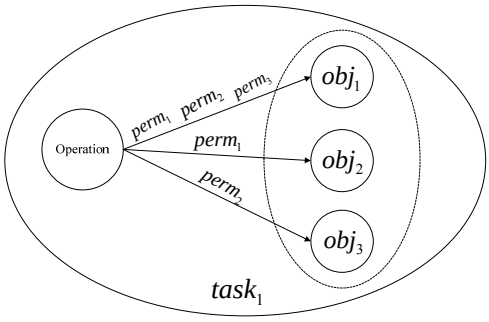


Figure 2. Task instance

For example, in a remote calibration system, a task named creating and editing calibration transaction file contains the view permission to an object named instrument information storing data and the view and edit permissions to an object named calibration transaction information storing data.

### B. Task-constraint-based Access Control

The task-constraint-based access control mode is expressed as (1).

$$TASK \rightarrow USER \times ROLE \times GC \times EC . \quad (1)$$

In (1), $USER = \{user_i | i = 1,2,3,...\}$, $ROLE = \{role_i | i = 1,2,3,...\}$, $GC = \{gc_i | i = 1,2,3,...\}$ and $EC = \{ec_i | i = 1,2,3,...\}$ represents user set, role set, authorization constraint set and execution constraint set, respectively. Equation (1) means: A user corresponds to a task set named $TASK_r$ according to the role named $r$ the user acts as; when authorizing a task named $tsk$ to a user named $u$, if the user $u$ satisfies the authorization constraint set named $GC_{u,tsk}$, then the authorization is successful, otherwise the authorization is fail; users can't abusing permission, they can use a permission only when the execution constraint set is satisfied, for example, the user $u$ can execute the task $tsk$ only when the execution constraint set named $EC_{u,tsk}$ is satisfied. In above, $TASK_r \subseteq TASK$, the value of it is related to the

role $r$; $GC_{u,tsk} \subseteq GC$, $EC_{u,tsk} \subseteq EC$, the value of them is related to the user $u$ and the task $tsk$.

Task, authorization constraint and execution constraint are the main characteristics which the task-constraint-based access control mode differs from other access control modes. The task-constraint-based access control defines authorization constraints and execution constrains by the characteristics of task and the relation among tasks. Authorization constraints ensure the principle of least privilege and the principle of separation of duty, and execution constraints ensure the principle of least privilege.

Authorization constraints include authorization responsibility constraint, authorization separation constraint, authorization count constraint and authorization time constraint. They are defined respectively as follows.

**Definition 2.** Authorization responsibility constraint, ARC for short: It means a user corresponds to a task set named $TASK_r$ according to the role named $r$ the user acts as, the task not in $TASK_r$ can't be authorized to the user. ARC is expressed as (2).

$$GC: TASK_r \rightarrow USER_r . \tag{2}$$

Equation (2) represents the user acts as the role $r$ only can be authorized the task in $TASK_r$. ARC is an authorization constraint based on task, and is controlled by the specific task in access control. It reflects the principle of least privilege.

**Definition 3.** Authorization separation constraint, ASC for short: It means the user who is authorized the task $tsk$ can't be authorized either task in $TASK_i$. ASC is expressed as (3).

$$GC: tsk \leftrightarrow TASK_i . \tag{3}$$

Equation (3) represents the task $tsk$ and either task in $TASK_i$ can't both be executed by the same user. ARC is an authorization constraint based on task too, and is controlled by the specific task in access control. It reflects the principle of separation of duty.

**Definition 4.** Authorization count constraint, ACC for short: It means the number of tasks which a user has can't be infinite. ACC is expressed as (4).

$$GC: user \leftarrow n . \tag{4}$$

Equation (4) represents the number of tasks which a user can be authorized is $n$ which doesn't include the number of completed tasks. ACC is an authorization constraint based on user, and is controlled by the specific user in access control. It prevents from expanding the permission of user infinitely and reflects the principle of least privilege.

**Definition 5.** Authorization time constraint, ATC for short: It means a task can be authorized to a user only at a time between a time interval. ATC is expressed as (5).

$$GC: task \leftarrow [t_{\min}, t_{\max}] . \tag{5}$$

In (5), $[t_{\min}, t_{\max}]$ represents a time interval, it consists of lower limit $t_{\min}$ and upper limit $t_{\max}$, and $t_{\min} \le t_{\max}$. Equation (5) represents a task can be authorized to a user only when the authorization time $t$ satisfies the condition $t_{\min} \le t \le t_{\max}$. ATC is an authorization constraint based on task, and is controlled by the specific task in access control. It prevents a user from obtaining a permission at any time which expands the permission of the user and reflects the principle of least privilege.

Execution constraints include execution lifetime constraint, execution sequence constraint and execution time constraint. They are defined respectively as follows.

**Definition 6.** Execution lifetime constraint, ELC for short: It means a user can execute a task only when the task is in running state.

The lifetime of task includes four states: dormant state, blocking state, running state and complete state, shown as Fig. 3. Each state is described as follows:

(1) Dormant state: It means the task has been created, but the task hasn't been assigned to a user.

(2) Blocking state: It means the task has been assigned to a user, but the user can't execute the task because the execution constraint set isn't satisfied.

(3) Running state: It means the task can be executed, the user who is authorized the task can execute it.

(4) Complete state: It means the task has been completed, no users can execute a completed task.

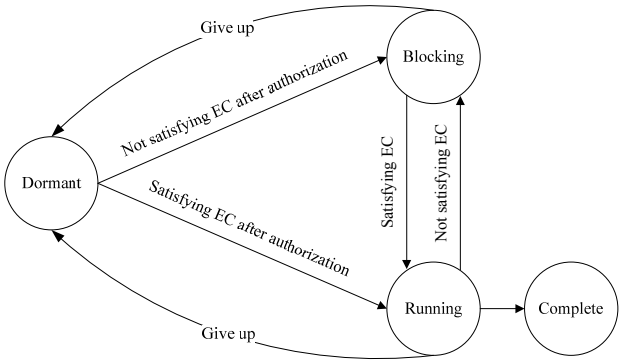


Figure 3. The lifetime of task

As shown in Fig. 3, the state transition of task is described as follows: The initial state when the task is created is dormant state; the state turns into running state if satisfying the execution constraint set after authorizing the task to a user, otherwise the state turns into blocking state; the state turns into blocking state if the task in running state doesn't satisfy the execution constraint set; if the user who is authorized the task can't complete the task for various reasons, the state of the task is reinitialized to the dormant state; the state turns into complete state if the task is completed.

ELC is a basic execution constraint, and is controlled by the system according to the state of task. ELC means a task can be executed only when it's in running state. It reflects the principle of least privilege.

**Definition 7.** Execution sequence constraint, ESC for short: It means a task $task_j$ can be executed only after another task $task_i$ has been completed. ESC is expressed as (6).

$$EC: task_i \Rightarrow task_j . \quad (6)$$

ESC is used to ensure the user execute the task in an ordered sequence. It limits the scope of user permission and reflects the principle of least privilege.

**Definition 8.** Execution time constraint, ETC for short: It means a task can be executed only at a time between a time interval. ETC is expressed as (7).

$$EC: task \leftarrow [t_{\min}, t_{\max}]. \quad (7)$$

Equation (7) represents a task can be executed only when the execution time $t$ satisfies the condition $t_{\min} \le t \le t_{\max}$. ETC is an execution constraint based on task, and is controlled by the specific task in access control. ETC prevents the user from abusing permission at any time which expands the permission of the user and reflects the principle of least privilege.

### C. TCBAC model

**Definition 9.** TCBAC model: $TCBAC = \{USER, ROLE, TASK, GC, EC, TU\}$. In the model, $USER$, $ROLE$, $TASK$, $GC$, $EC$, $UR$, $TU$ represents user set, role set, task set, authorization constraint set, execution constraint set, user and role assignment relation, task authorization mechanism. Fig. 4 is the TCBAC model schematic diagram, where $TASK_N$ is the task set which hasn't been assigned and $TASK_A$ is the task set which has been assigned.

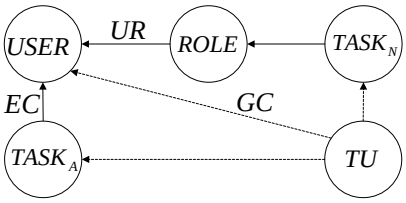


Figure 4. TCBAC model

The running of TCBAC is based on three relations and one mechanism.

(1) User and role assignment relation $UR$: It means the relation between user and role, the user corresponds to a task set according to the role the user acts as in the system. $UR$ is expressed as (8).

$$UR: ROLE \rightarrow USER . \quad (8)$$

(2) User and task authorization constraint relation $GC$: It means a user can't obtaining task permission arbitrarily and the user can obtain task permission only when the $GC$ is satisfied, reflects the principle of least privilege and the principle of separation of duty. $GC$ mainly includes ARC, ASC, ACC and ATC, is expressed as (9).

$$GC = \{ARC, ASC, ACC, ATC\}. \quad (9)$$

(3) User and task execution constraint relation $EC$: It means a user can't abusing task permission and the user can execute a task only when the $EC$ is satisfied, reflects the principle of least privilege. $EC$ mainly includes ELC, ESC and ETC, is expressed as (10).

$$EC = \{ELC, ESC, ETC\}. \quad (10)$$

(4) Task authorization mechanism $TU$: It realizes to build the one to one relation between task and user, is expressed as (11).

$$TU: TASK \rightarrow USER . \quad (11)$$

The implementation algorithm for TCBAC model is expressed as Algorithm 1.

**Algorithm 1**: The pseudo-code of implementation algorithm for TCBAC model

```
1 DefiningRole(); // Defining role
2 DefiningUser(); // Defining user
3 DefiningUR (); // User and role assignment
4 DefiningTask(); // Defining task
5 DefiningGCofUser(user[i]); // Defining authorization
  constraints based on user, such as ACC
6 DefiningGCofTask(task[i]); // Defining authorization
  constraints based on task, such as ACC, ATC
7 DefiningECofTask(task[i]); // Defining execution
  constraints based on task, such as ESC, ETC
8 TU(); // Task authorization
9 ExecutingTask(task[i]); // Executing a task if the
  execution constraint set is satisfied
```

## IV. Application and Analysis of TCBAC in Remote Calibration System

TCBAC is applied in a remote calibration system in this section. The application method of TCBAC in the remote calibration system is described in detail, and the performance of TCBAC is analyzed.

### A. Role, User and UR Relation Definition

Combining with the structure of remote calibration system, four roles which are administrator of metrology institution, ordinary staff of metrology institution, administrator of calibration customer and ordinary staff of calibration customer are set in remote calibration system. The distribution of the four roles in remote calibration system is shown as Fig. 5.

In metrology institution, one administrator and some

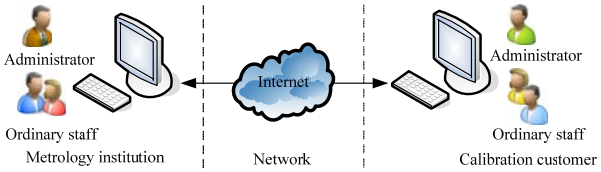


Figure 5. The roles of remote calibration system

ordinary staffs are set. For each calibration customer, one administrator and some ordinary staffs are set too. The administrator account of metrology institution is configured directly by the system, and the ordinary staff account of metrology institution can be configured by the administrator of metrology institution or be generated by registering independently. The administrator account and ordinary staff account of calibration customer are generated by the mechanism of registering independently and auditing by the ordinary staff of metrology institution. The user and role assignment relation is configured automatically by the system when a user registers. A user only can act as one role.

### *B. Definition of Task, GC and EC*

GC based on user is shown in Table I, including ARC and ACC. The task definition of the system is shown in ARC in detail.

TABLE I.
GC BASED ON USER

| Role | ARC | ACC |
|---|---|---|
| Administrator of metrology institution | (1)Ordinary staff register (2)Modifying user information (3)Viewing user information (4)Viewing issued certificate (5)Confirming calibration application (6)Issuing calibration certificate (7)Viewing the detailed information of calibration order in progress | None |
| Ordinary staff of metrology institution | (1)Auditing register information (2)Viewing user information (3)Viewing instrument information (4)Adding standard instrument information (5)Viewing standard instrument (6)Adding command file of standard instrument (7)Adding calibration transaction file (8)Viewing calibration transaction file (9)Calibration operations: ①Viewing calibration customer ②Viewing calibrated instrument ③Selecting standard instrument ④Confirming standard instrument ⑤Creating and editing calibration transaction file ⑥Confirming calibration transaction file ⑦Auditing calibration process for the first time ⑧Auditing calibration process for the second time ⑨Drawing conclusion | It's set according to specific situation, such as 10. |
| Administrator of calibration customer | (1)Company register (2)Ordinary staff register (3)Modifying staff information (4)Viewing staff information (5)Viewing instrument information (6)Making calibration application (7)Viewing calibration result (8)Printing calibration certificate | None |
| Ordinary staff of calibration customer | (1)Modifying personal information (2)Adding instrument information (3)Viewing instrument information (4)Adding instrument command file (5)Calibration operations: ①Viewing calibrated instrument information ②Executing calibration transaction file ③Confirming calibration operation | It's set according to specific situation, such as 5. |

GC and EC based on task are shown in Table II. Only the tasks have GC and EC are shown, and the tasks which aren't shown have no authorization constraints and execution constraints. The constraint based on task includes ASC, ATC, ELC, ESC and ETC.

### *C. Access Control Implementation Process of TCBAC*

For a remote calibration operation in the remote calibration system, the access control implementation process of TCBAC is described as follows:

(1) The administrator of calibration customer executes the task of making calibration application which submits a calibration application to the metrology institution.

(2) The administrator of metrology institution receives the calibration application and executes the task of confirming calibration application. When the calibration application is confirmed, the tasks which the calibration application includes are broadcasted to the ordinary staffs of metrology institution and the ordinary staffs of calibration customer under the constraint of ARC.

(3) The ordinary staffs of metrology institution and the ordinary staffs of calibration customer can obtain the tasks which are broadcasted to them under the constraints of ASC and ATC.

(4) The ordinary staffs of metrology institution and the ordinary staffs of calibration customer can execute the tasks which they have obtained under the constraints of ELC, ESC and ETC.

### *D. Performance Analysis of TCBAC*

The effects of using TCBAC in remote calibration system are summarized. Then TCBAC is compared with DAC, MAC and RBAC which are commonly used access control models at present. The comparison results are shown in Table III.

The comparison result shown in Table III is explained as follows:

(1) TCBAC conducts the fine granularity access control according to calibration task from task perspective, and considers the dynamic change of task and context, so it has good safety, satisfies the principle of least privilege and the principle of separation of duty and has good expansibility.

(2) DAC, MAC and RBAC are static access control models, don't consider context and haven't dynamics.

(3) User can delegate permissions independently in DAC, so DAC has good authorization flexibility. But it's easy to make safety out of control, can't satisfy the principle of least privilege.

TABLE II.
GC AND EC BASED ON TASK

| Role | Number | Task | ASC | ATC | ELC | ESC | ETC |
|---|---|---|---|---|---|---|---|
| Ordinary staff of metrology institution | 1 | Viewing calibration customer information | None | None | Automation | None | None |
| | 2 | Viewing calibrated instrument information | None | None | Automation | None | None |
| | 3 | Selecting standard instrument | None | According to need | Automation | None | According to need |
| | 4 | Confirming standard instrument | None | According to need | Automation | Task 3 | According to need |
| | 5 | Creating and editing calibration transaction file | None | According to need | Automation | Task 4 | According to need |
| | 6 | Confirming calibration transaction file | None | According to need | Automation | Task 5 | According to need |
| | 7 | Auditing calibration process for the first time | Task 8 | According to need | Automation | Task 11 | According to need |
| | 8 | Auditing calibration process for the second time | Task 7 | According to need | Automation | Task 7 | According to need |
| | 9 | Drawing conclusion | Task 7 and Task 8 | According to need | Automation | Task 8 | According to need |
| Ordinary staff of calibration customer | 10 | Viewing calibrated instrument information | None | According to need | Automation | None | According to need |
| | 11 | Executing calibration transaction file | Task 12 | According to need | Automation | Task 6 | According to need |
| | 12 | Confirming calibration operation | Task 11 | According to need | Automation | Task 11 | According to need |

TABLE III.
THE COMPARISON RESULT AMONG TCBAC, DAC, MAC AND RBAC

| Access control model | Security | Least privilege | Separation of duty | Dynamics | Context | Expansibility |
|---|---|---|---|---|---|---|
| TCBAC | √ | √ | √ | √ | √ | √ |
| DAC | √ | | | | | √ |
| MAC | √ | √ | | | | |
| RBAC | √ | | √ | | | √ |

(4) MAC takes the method of mandatory access control, has good safety. But its authorization isn't flexible and its expansibility is poor.

(5) RBAC has good safety, good authorization flexibility and good expansibility. But it doesn't consider context and dynamics, can't satisfy the principle of least privilege.

## V. CONCLUSION

A task-constraint-based access control model named TCBAC for remote calibration is presented in this paper. The model has the characteristics and advantages as follows:

(1) TCBAC conducts the fine granularity access control according to calibration task, defines authorization constraints and execution constraints by the characteristics of task and the relation among tasks. User can obtain a task permission only when the authorization constraint is satisfied and execute a task only when the execution constraint is satisfied. Authorization constraints and execution constraints ensure the principle of least privilege and the principle of separation of duty together.

(2) Comparing with DAC, MAC and RBAC which are commonly used access control models at present, TCBAC has the advantages of considering context and dynamics, it more fully satisfies the principle of least privilege and the principle of separation of duty and has good expansibility.

The authorization mechanism of TCBAC model will be further researched in the future in order to improve the practicability of TCBAC model.

## ACKNOWLEDGMENT

This work was partially supported by the New Century Excellent Researcher Award Program from Ministry of Education of China (NCET-08-0211).

## REFERENCES


[1] Yu Zhang, Jing Zu, and Dongxing Pei, "The miniature internal electronic pressure gauge and dynamic calibration method," Journal of Computers, vol. 7, no. 11, pp. 2750-2757, 2012.

[2] Xiaobin Hong, Guixiong Liu, Zhuokui Wu, and Xipeng Du, "Remote calibration system for frequency based on in-place benchmark," Frontiers of Mechanical Engineering, vol. 5, no. 3, pp. 316-321, 2010.

[3] M. Helmy A. Raouf, Rasha S. M. Ali, and M. S. Gadelrab, "Construction and remote calibration of an automated resistance measuring system," MAPAN, vol. 26, no. 2, pp. 125-131, 2011.

[4] S. Matsuzawa, T. Shimodaira, K. Hanaoka, A. Shimoyama, S. Sakagami, A. Domae, et al., "Feasibility study on remote calibration of impedance standard for industrial use,", 2008 Conference on Precision Electromagnetic Measurements Digest, pp. 348-349, 2008.

[5] Tokihiko Kobata, Momoko Kojima, and Hiroaki Kajikawa, "Development of remote calibration system for pressure standard," Measurement, vol. 45, no. 10, pp. 2482–2485, 2012.

[6] Yue Qi and Heng Wang, "Thermocouple thermometer remote calibration system design," Metrology & Measurement Technique, vol. 39, no.2, pp. 14-15, 2012.

[7] Jingtao Guo and Zhigang Jin, "General tele-calibration platform based on Internet," Chinese Journal of Scientific Instrument, vol. 32, no. 4, pp. 932-940 2011.

[8] Guoyuan Lin, Yuyu Bie, and Min Lei, "Trust based access control policy in multi-domain of cloud computing," Journal of Computers, vol. 8, no. 5, pp. 1357-1365, 2013.

[9] Fenghua Li, Mang Su, Guozhen Shi, and Jianfeng Ma, "Research status and development trends of access control model," ACTA Electronica Sinica, vol. 40, no. 4, pp. 805-813, 2012.

[10] Zan Yang, Lin Yang, Xiangyang Luo, Linru Ma, Baosheng Kou, and Kun Zhang, "Model of domain based RBAC and supporting technologies," Journal of Computers, vol. 8, no. 5, pp. 1220-1229, 2013.



**Zhuokui Wu** was born in 1980, is currently a lecturer in Zhongkai University of Agriculture and Engineering, Guangzhou, China. He received master degree from South China University of Technology, Guangzhou, China, in 2006. He is currently pursuing doctor degree at School of Mechanical & Automotive Engineering in South China University of Technology. His research interests include information system, instrument, measurement and control technology.

**Guixiong Liu** was born in 1968, is currently a professor and doctoral supervisor in South China University of Technology, Guangzhou, China. He received doctor degree from Chongqing University, Chongqing, China, in 1995. His research interests include modern detection technology and networked control, intelligent sensing theory and method, information system modeling theory and application.