International Journal of Security and Its Applications
Vol. 10, No. 2 (2016), pp.85-94
http://dx.doi.org/10.14257/ijsia.2016.10.2.08

Research on the Strategy of Role Management Based on Grid Environment

Yi He LIU[1,a],Yu Ping QIN[2,b],Shuang ZHANG[1,2,3,c]

[1] *College of computer science,Neijiang Normal University, Neijiang,641000,china*
[2] *The engineering & technical college of chengdu university of technology, Leshan,614000,china*
[3] *University of Macau, Taipa,Macau,999078 China.*
E-mail: [a]*liu_yihe@163.com;* [b]*qin_yp@yeah.net;*[c]*zhangshuanghua1@126.com*

Abstract

The grid security affects directly the development of the grid and the practical application of grid system software. The access control is one of important contents of grid security research. The traditional access control models have ignored the subject security, and can not be solved with the dynamic grid, and the characteristics of the coexistence of multiple security strategy etc problems. Regarding expanded the concepts under the common network environment subject, the object, safe service, granularity control, the concept of subject/ object decomposition and the organization classifications are defined. Using the RBAC model and BLP the model basic principle, some of the new access control security strategy based on the grid environment has been defined in the paper. After discussion shows that the new rules emphasis on the subject security, and adapt to the dynamic nature of grid environment and characteristics of the coexistence of multiple security strategy. The new rules are compatibility with existing network access control model, they are secure and are also an expansion under the common network environment access control strategy, and this has certain positive significance to the grid security research.

Keywords*: Grid Security, BLP Model, RBAC Model, Access Control Strategy*

1. Introduction

With the rapid development of internet technology, The security of grid has become the direction of future research scientists, the grid biggest problem is how to safeguard the security of grid environment, grid security in the grid system plays a decisive role, the grid needs a good environment for a very strong security requirements, this requirement is for the grid environment thorough a variety of security policy studies. The current grid security research focuses on the security grid authentication, access control, data integrity, communication confidentiality, the undeniable user behavior, as well as single sign-on and so on [2-5], what this article discusses is the access control question based on grid environment.

Because the characteristics of the grid itself, the access control model applied originally in the traditional network is very difficult to directly in the new grid environment to use, and that is unable to meet the grid environment characterized by the coexistence of diverse security policies etc[6] . The access control features for grid environment have studied in many literatures. For instance, the access control are discussed based on grid security infrastructure in literatures [6,7], based on agents of the grid environment with a typical access control model of network environment in literature [8], and in literature [9], etc. Although these literatures have studied under the grid environment access control question, but most only involves on the one hand, considered

ISSN: 1738-9976 IJSIA

that grid characteristics and so on environment dynamic and multi-securities are insufficient. In literatures [10], using RBAC model [11] and BLP the model [12] basic property, and using grid environment characteristic, some new access control strategies are described under the stress discussion grid environment, and the strategies as far as possible adaptive grid environment of the dynamic and the multi-securities. In this article, we will use the idea of RBAC model, from the perspective of role management, to improve the existing access control strategies, and make it more adapt to the grid environment.

The paper following part organizations are as follows. The 2nd section introduces the existing related concept and the known basic security model. The 3rd section first gives to carry on the new concept for the strategy description introduction. Next gives the concepts of the expansion subject and object, safe service, control granularity and so on. Finally gives the main safety strategy description and the example. The 4th section gives the strategy the secure discussion. The 5th section gives the article the summary.

2.Related Concept

2.1. Grid and Grid Security

In the grid environment, different autonomous domains or virtual organizations compose the entire grid computation environment to be able to provide the outward service. The resources of resources node of each autonomous domain or virtual organization can cooperate to complete the different service, if the grid user submitted tasks that can not be completed in an autonomous domain or virtual organization, then the server of this autonomous domains or virtual organizations can requested that resources node of other autonomous domains or virtual organizations cooperation complete. Figure 1 [13] shows the physical view of grid security.

This article carries on the discussion take the GSI security strategy [1, 14] in grid globus environment as the foundation.

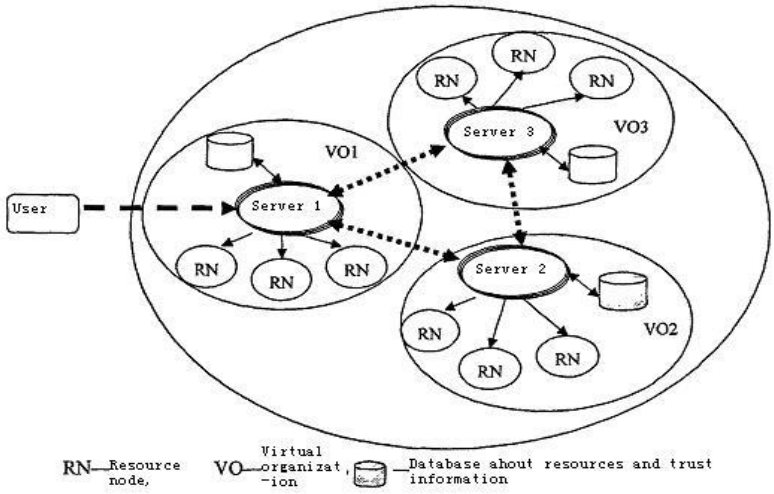

Figure 1. The Physical View of Grid Security

2.2. Basic Concept

Subject and object: calculator inside the operation that esse large quantity involve the safety, any puts to operate into practice of call the subject , with $s_1,s_2,\ldots,s_i,\ldots$,or s indicated ,and its gather to mean with S. Object that were called by operation , with $o_1,o_2,\ldots,o_j,\ldots$,or o indicated ,and its gather to mean with O.

We suppose there are m virtual organizations in the entire grid globus environment in this paper, a subject represents a user or the user process in this environment. The virtual organizations VO_i corresponding the local resources subject set are denoted with S_VO_i , the corresponding local resources object set are denoted with O_VO_i（i=1,2,…m）.

When the subject s needs simultaneously to access the virtual organization VO_1,$VO_{2,}$…,VO_m, the resources proxy need to a globus subject be mapped to the subject of one or more of local resources. We said s'decomposition expression in a virtual organization, with s=(s_VO_1,s_VO_2,…,s_VO_m), in which the jth component expresses the globus subject mapping for the jth virtual organization's subject , such as the s does not need maps to the virtual organization VO_j , then note the corresponding components for the $s\_VO_j\_\varphi$（j=1,2,..,m）[10].

When object o needs to decompose to virtual organization VO_1, VO_2…VO_m complete, said that o decomposes expression in the virtual organization is o=(o_VO_1, o_VO_2,…, o_VO_m), in which the jth component is that the object o decomposes into the part of virtual organization VO_j , and if the object o do not needs to decompose to virtual organization VO_j, then we records the corresponding component for $o_j\_VO_j\_\varphi$ (j=1,2. , m).

Classification: in this paper, classifications (confidentiality grade) of the subject and object are in a specific way measure to reference the paper [15]. Confidentiality grade of subject s is denoted with T(s),and confidentiality grade of object o is denoted with T(o).

What needs to explain is the definition of the classifications function using what methods, there is no influence for behind of discussion.

If the grid user submitted tasks that cannot be completed in an autonomous domain or virtual organization, then the server of this autonomous domains or virtual organizations can requested that resources node of other autonomous domains or virtual organizations cooperation completes.

For simplicity, this note: $s\_VO_j \in S\_VO_j$, said that the globus subject s has been mapped to the subject having the local nature of virtual organization VO_j. Specific mapping strategy can be found in the paper [14], do not discuss here (j = 1,2, .., m).

When a subject or an object not in a virtual organization, with decomposition expression, the classifications T(s) /T (o) of subject s /object o is a vector function, in which component's definition can be defined to imitate in the common network environment related definition, for example: T(s)=(T(s_VO_1),T(s_VO_2),…,T(s_VO_m)).

2.3. Basic Security Model

According to BLP model [12], system is at a secure status (confidentiality), need to satisfy: do not read up, do not write down, that is:

If $T(s) \geq T(o)$ then subject s can read object o ,and if $T(s) \leq T(o)$ then subject s can write object o.

The basic idea of RBAC model [11] is the division of responsibility, which is very similar to an organization. In the RBAC model, users are granted roles, roles are granted permissions, the permissions associated with operating. Users are granted the role to be the role appropriate permissions to complete the some operations. We will take the concepts of basic RBAC model in this paper.

Below take most basic nature of the RBAC model as the basis, some related symbols are given.

System has a role set denoted R, make R={r_1,r_2,…,r_n}. All roles corresponding permission set is denoted R_P, make R_P={p_1,p_2,…,p_m}.A role set which subject s owned is denoted SR(s). A subject set which role r corresponds to is denoted: RS(r). A role set which object o owned is denoted: OR(o). An object set which role r corresponds to is denoted: RO(r). A right set which role r corresponds to is denoted: RP (r). A permission set which s owned based role is denoted SP(s). A permission set which object o is allowed to use and based role denoted: OP(o).

3.New Access Control Strategies Based Grid Environment

3.1. New definition

In order to give the access control strategy of the subject and object under the grid environment, we give some new definitions in the following.

3.1.1. Rule and Permission Decomposition

Rule decomposition: when the subject s needs simultaneously to access the virtual organization VO_1 、 VO_2…VO_m, We said s'decomposition expression in virtual organization, with s=(s_VO_1,s_VO_2,…,s_VO_m), The decomposition expression of rule r in virtual organization, is denoted with r=(r_VO_1,r_VO_2,…,r_VO_m).

Permission p decomposition:the decomposition expression of a permission p in virtual organization, is denoted with p=(p_VO_1,p_VO_2,…,p_VO_m).

When the r or p does not need maps to the virtual organization VO_j , then note the corresponding components for the r_VO_j_φ or p_VO_j_φ（j=1,2,..,m）.

3.1.2. Set Decomposition

Similar to the previously described decomposition of a single element, we generalize to the set. Such as role set R, which decomposition in a grid environment referred to as: R = (R_VO_1, R_VO_2, ..., R_VO_m), wherein R_VO_j,(j =1,2 , ..., m) represents the set of all the roles that are decomposed in a virtual organization VO_j When the R does not need maps to the virtual organization VO_j , then note the corresponding components for the R_VO_j_φ（j=1,2,..,m）.

3.2. New Access Control Srategies

The access mode that subject s from the security angle consideration visits to object o is denoted with access_mode(s, o).The value range of access_mode(s, o) is a permission set, in which s takes a user, when plays a role, simultaneously considered that the BLP model correspondence the safe limit, carries on the operation to o, and it is actually a subset of R_P, which should contain re: read, w: write, c: create; d: delete etc such permission.

In this way, the safety factors of subject s have s,T(s), SR(s),s_sa,s_rg,s_fg etc. The safety factors of object o have o,T(o),OR(o),o_sa,o_rg,o_fg etc. Here s_sa or o_sa are respectively a sub-set of security services set (denoted as: P) in grid environment. The s_rg and s_fg are respectively the roughly granularity set and fine granularity set of object subject s The o_rg and o_fg are respectively the roughly granularity set and fine granularity set of object o [15].

It is assumed that when the initial conditions does not involve the rule management and used BLP model, the whole grid environment is safe, namely, information transmission and other areas are safe.

3.2.1. Create a role Strategy

Creat_role(s，T(s)，SR(s)，s_sa，s_rg，s_fg：r，RS(r)，RP(r)，RO(r))，SP(s)，OP(o)，OR(o) // The subject s increases the role r for the whole system, wherein the subject s have security attributes that are T(s)， SR(s)，s_sa，s_rg，s_fg etc. The rule r are correspond to the subject set for RS(r), to the permissions set for RP(r) ,and object set RO(r) etc

If s_sa⊄P or s_rg ⊄P_rg or s_fg⊄ P_fg or c∉ SP(s) then go_end// The system does not provide the s security service, or s does not meet the coarse-grained or fine-grained rules of sytsem ,or s without creating the role right, end

R=R∪{r} // Refresh rule r and its decomposition
For j=1 to m
R_VO_j= R_VO_j ∪{ r_VO_j }
Endfor
∀ r’ ∈R， R_P=R_P ∪RP(r)// Refresh the permission set of rule r corresponding to ,and the decomposition of the permission set
For j=1 to m
$R\_P\_VO_j$= $R\_P\_VO_j$ ∪{ $PR(r\_VO_j)$}
Endfor
∀ s’ ∈RS(r)， SR(s’)=SR(s’) ∪{r} // Refresh the rule set of the subject owning ,and the decomposition of the rule set
For j=1 to m
$SR(s'\_VO_j)$= $SR(s'\_VO_j)$ ∪{ r_VO_j }
Endfor
∀ s’ ∈RS(r)， SP(s’)=SP(s’) ∪RP(r)// Refresh the permission set of the subject owning the rule r ,and the decomposition of the permission set
For j=1 to m
$SP(s'\_VO_j)$= $SP(s'\_VO_j)$∪{ $PR(r\_VO_j)$}
Endfor
∀ o’ ∈RO(r)， OR(o’)=OR(o’)∪{r} //Refresh the rule set of the object owning ,and the decomposition of the rule set
For j=1 to m
$OR(o'\_VO_j)$= $OR(o'\_VO_j)$∪{ r_VO_j }
Endfor
∀ o’ ∈RO(r)， OP(o’)=OP(o’) ∪RP(r)// Refresh the permission set of the object owning rule r ,and the decomposition of the permission set
For j=1 to m
$OP(o'\_VO_j)$= $OP(o'\_VO_j)$∪{ $PR(r\_VO_j)$ }
Endfor
// According to the new role set , to make the corresponding pattern adjustment visit to all possible
∀ s ∈S， ∀ o∈O，access_model(s，o)＝SP(s)∩OP(o)
For j=1 to m
For j=1 to m
$access\_model(s\_VO_i, o\_VO_j) = SP(s\_VO_i) \cap OP(o\_VO_j)$
Endfor
Endfor
DO CASE // For any s, o, the T(s), T(o) are discussed in different situations
CASE T(s) >T(o)
If {w}∈access_model(s，o) then access_model(s，o)＝access_model(s，o)－{w} // Remove the w right, to the end.
For j=1 to m
For j=1 to m
If {w}∈$access\_model(s\_VO_i, o\_VO_j)$ then $access\_model(s\_VO_i, o\_VO_j)$ ＝$access\_model(s\_VO_i, o\_VO_j)$－{w} // Remove the w right, to the end.
Endfor
Endfor
CASE T(s) <T(o)
If {re}∈access_model(s，o) then access_model(s，o)＝access_model(s，o)－{re}// Remove the re right, to the end.
For j=1 to m
For j=1 to m

If {re}∈access_model(s_VO_i， o_VO_j) then access_model(s_VO_i， o_VO_j) ＝access_model(s_VO_i， o_VO_j)－{re} // Remove the re right, to the end.
Endfor
Endfor
ENDCASE

3.2.2. Delete a role strategy

Delete_role(s，T(s)，SR(s)，s_sa，s_rg，s_fg：r，RS(r)，RP(r)，RO(r))，SP(s)，OP(o)，OR(o) // The subject s delete the role r for the whole system, wherein the subject s have security attributes that are T(s)，SR(s)，s_sa，s_rg，s_fg etc. The rule r are correspond to the subject set for RS(r), to the permissions set for RP(r) ,and object set RO(r) etc

If $s\_sa \not\subset P$ or $s\_rg \not\subset P\_rg$ or $s\_fg \not\subset P\_fg$ or $c \notin SP(s)$ then go_end// The system does not provide the s security service, or s does not meet the coarse-grained or fine-grained rules of sytsem ,or s without deleting the role right, end

If $s\_sa \not\subset P$ or $s\_rg \not\subset P\_rg$ or $s\_fg \not\subset P\_fg$ or $d \notin SP(s)$ then go_end// If s without corresponding security attributes, to the end

$\forall$ s’ ∈RS(r)，SR(s’)=SR(s’)－{r} //Refresh the rule set of the subject owned ,and the decomposition of the rule set

For j=1 to m
$SR(s'\_VO_j)= SR(s'\_VO_j) －\{ r\_VO_j \}$
Endfor

$\forall$ o’ ∈RO(r)，OR(o’)=OR(o’)－{r} // Refresh the rule set of the object owned , and the decomposition of the rule set

For j=1 to m
$OR(o'\_VO_j)= OR(o'\_VO_j) －\{ r\_VO_j \}$
Endfor

R=R－{r}// Refresh the rule set and its decomposition

For j=1 to m
$R\_VO_j= R\_VO_j －\{ r\_VO_j \}$
Endfor

$\forall$ r’ ∈R， R_P=$\cup$RP(r’)//Refresh the permission set of system and its decomposition

For j=1 to m
$R\_P\_VO_j=\cup R\_P(r'\_VO_j)$
Endfor

$\forall$ s’ ∈S，SP(s’)=$\cup_{r' \in SR(s')} RP(r')$ //Refresh the permission set of subject ,and the decomposition of the permission set

For j=1 to m
$SP(s'\_VO_j) = \cup_{r'\_vo_j \in SR(s'\_VO_j)} RP(r'\_VO_j)$
Endfor

$\forall$ o∈O，OP(o)=$\cup_{r' \in OR(o)} RP(r')$ // Refresh the permission set of object , and the decomposition of the permission set

For j=1 to m
$OP(o\_VO_j) = \cup_{r'\_vo_j \in OR(o\_VO_j)} RP(r'\_VO_j)$
Endfor

RS(r)=RO(r)=RP(r)= Φ

For j=1 to m

$RS(r\_VO_j)=RO(r\_VO_j)= RP(r\_VO_j)= \Phi$

Endfor

$\forall$ s $\in$S, $\forall$ o$\in$O,access_model(s,o)＝SP(s)$\cap$OP(o) //The following discussion is the same with that discussion of section 3.2.1, here omitted

3.2.3. Assign Permissions to Roles

Append_ purview(s，T(s)，SR(s)，s_sa，s_rg，s_fg：r，RS(r)，RP(r)，RO(r)，p, SP(s)，OP(o)) //The subject s increases powers p for rule r. The subject s have security attributes that are T(s)，SR(s)，s_sa，s_rg，s_fg.The original rule r corresponding to subject set, permissions set and object set is respectively RS(r),RP(r) and RO(r) etc

If s_sa$\not\subset$P or s_rg $\not\subset$P_rg or s_fg$\not\subset$ P_fg or c$\notin$ SP(s) then go_end // If s without corresponding security attributes, to the end

RP(r)=RP(r) $\cup${p}// Refresh the permission set of rule r ,and the decomposition of the permission set

For j=1 to m

$RP(r\_VO_j)= RP(r\_VO_j)\cup\{ p\_VO_j \}$

Endfor

$\forall$ r’ $\in$R，R_P=$\cup$RP(r’)/ Refresh the permission set of system and its decomposition

For j=1 to m

$R\_P\ \_VO_j=\cup RP(r\_VO_j)\}$

Endfor

$\forall$ s’ $\in$RS(r)，SP(s’)=SP(s’) $\cup$RP(r)// Refresh the permission set of the subject owning the rule r ,and the decomposition of the permission set

For j=1 to m

$SP(s'\ \_VO_j)= SP(s'\ \_VO_j)\cup\{ PR(r\_VO_j)\}$

Endfor

$\forall$ o’ $\in$RO(r)，OP(o’)=OP(o’) $\cup$RP(r)// Refresh the permission set of the object owning rule r ,and the decomposition of the permission set

For j=1 to m

$OP(o'\_VO_j)= OP(o'\_VO_j)\cup\{ PR(r\_VO_j) \}$

Endfor

$\forall$ s $\in$S，$\forall$ o$\in$O，access_model(s，o)＝SP(s)$\cap$OP(o) //The following discussion is the same with that discussion of section 3.2.1, here omitted

3.2.4 Delete the Permission of a role

Delete_ purview(s，T(s)，SR(s)，s_sa，s_rg，s_fg：r，RS(r)，RP(r)，RO(r)，p, SP(s)，OP(o)) // The subject s will delete the permission p of the role r The subject s has security attributes that are T(s)，I(s)，SR(s)，s_sa，s_rg，s_fg. The original rule r corresponding to subject set, permissions set and object set is respectively RS(r),RP(r) and RO(r). wherein the group have security attributes that are RUS(r)，SUP(s)，OUR(o)，RUP（r）etc

If s_sa$\not\subset$P or s_rg $\not\subset$P_rg or s_fg$\not\subset$ P_fg or d$\notin$ SP(s)then go_end// If s without corresponding security attributes, to the end

RP(r)=RP(r)－{p}

//The following discussion is the same with that discussion of section 3.2.3, here omitted

4. Some Security Discussion of New Access Control Strategy

The access control strategies that are defined in this paper have the following some characteristics.

1）Used waiting for the processing subject number limit to enter the system subject number.

2）Used s_sa and o_sa set describe the subject and the object whether to have the safe service which the grid environment provides (for example authentication, encryption and so on).

3）When the subject and the object need to decompose to each virtual organization, pass through each roughly granularity set and fine granularity set of the virtual organization to control.

4）When s, o are decomposition, carries on the preliminary judgment step by step with the organization classification.

5）When s, o are decomposition, it is essential that the role set/ the permission set what subject s own is a subset of the role set / the permission set what object o has.

6）When s, o are decomposition, it is essential to judgment step by step with the rules of BLP model

From the characteristics above new access control strategies, these strategies have given dual attention to the classics RBAC model, the BLP model nature, have considered the subject multi-securities, the grid environment's dynamic, and have the diverse security policy coexisting characteristic.

5.Conclusion

In view of the traditional network access control strategy's existence insufficiency, the characteristics of common network environment are used, and based on the grid security's essential factor, many concepts have been defined or expanded in this article. They are the subject /object decomposition expression, organization classification, safe service, and granularity control so on. Used new concepts and basic principle of the RBAC model and of the BLP model, some new access control security strategies under grid environment are given. Through the analysis, these strategies have given dual attention to the classics RBAC model, the BLP model nature, have overcome the insufficiency of access control strategies under network environment, and have carried on the development. They are safe and reasonable access control strategies based on the grid environment, this has certain positive sense to the grid security research.

As the grid is too complicated, this paper is only limited to some description of typical strategies, will further construct and consummate other strategies from now on, and conduct the simulation research gradually.

Acknowledgment

This work is supported by Sichuan provincial science and technology department to apply basic research program (2015JY0119). Sichuan province academic and technical leader training funded projects (12XSJS002,13XSJS002) . Sichuan province department of education natural science point item 13ZA0003,14ZB0360,14ZB0363.

References

[1] Joshy Joseph, Craig Fellenstein .Grid comupte. Tsinghua University Press，**(2005)**.

[2] JIN nan. The grid safe authentication key technologies studies. Nanjing Posts and telecommunications University master's degree paper, in Chinese,**(2006).**

[3] May Phyo Oo, Thinn Thu Naing. Access Control System for Grid Security Infrastructure. IN Proceedings of IEEE/WIC/ACM International Conferences on Web Intelligence and Intelligent Agent Technology – Workshops. pages 299-302,(2007).

[4] HAN bing.study on data management and the security problem Under the grid environment. Chinese Scientific and Technical University master's degree paper,in Chinese, **(2006).**
[5] Xiaoqin Huangetc.An Identity-Based Model for Grid Security Infrastructure,IN Proceedings of ISSADS2005, pages 258-266,**(2005).**
[6] ZHANG Yifan. Study on access control based on the grid security infrastructure. South central national university master's degree paper, in Chinese,**(2009).**
[7] Welch V, Siebenlist F, Foster I. Security for Grid services. IN Proceedings of 12th IEEE International Symposium on High Performance Distributed Computing, papes.48-57,**(2003).**
[8] ZHANG Dongli. Grid security certain question research--Based on proxy access control system plan. Shanghai Jiaotong University Master's degree paper, in Chinese, **(2005).**
[9] MIN Rui. Grid safe access control engineering research. Hubei Industrial university master's degree paper, in Chinese, **(2008).**
[10] LIU yihe.Research on Access Control Based Grid Environment Journal of Computational Information Systems, 6(13):4503-4512. **(2010)**
[11] Sandhu RS, Samarati P. Access control: principles and practice.IEEE communications.32(9):40-48,**(1994).**
[12] Bell D E,Lapadula LJ.Secure compter system. Mathematical foundation.MTR-2527,Mitrecorp,Bedford,MA, **(1973).**
[13] WANG Fang. study Under the grid environment's trust mechanism. Nanjing Posts and telecommunications University master's degree paper, in Chinese,**(2009).**
[14] The Globus Project.http://www.globus.org/.
[15] Liu yihe.Model Research Based On Security Architecture Of Application Area Boundary.Sichuan university [Phd thesis],in Chinese,**(2005).**

Authors

Yi He LIU, He received the Ph.D. degree in Sichuan University,chengdu,sichuan, Chengdu,Sichuan,China, in 2005.

Since 2000, he has been involved in research in the areas of Direction of computer application technology , information security and intra-body communication.He is currently an Professor and the Head of the Faculty of computer science,The Neijiang Normal University,Neijiang,Sichuan,China.

Yu Ping QIN, She received the Master degree in Sichuan Normal University, chengdu,Sichuan, china, in 2011.

Since 2011, he has been involved in research in the areas of digital signal processing ,intra-body communication and cryptography.He is currently an Lecturer Department of basic courses,The engineering & technical college of chengdu university of technology, leshan,Sichuan,china.

Shuang ZHANG, He received the Master degree in Graduate University of Chinese Academy of Sciences, beijing, china, in 2011. He is currently working toward the Ph.D. degree from the Department of Electrical and Electronics Engineering, Faculty of Science and Technology, University of Macau, Taipa,Macau, China.

Since 2011, he has been involved in research in the areas of biomedical engineering , Digital signal processing (DSP) and information security. He is currently an Associate Professor Department of Electronic information and computer engineering,The engineering & technical college of chengdu university of technology, leshan,Sichuan, china;and Faculty of computer science,The Neijiang Normal University,Neijiang,Sichuan,China.