협업 환경 내 신뢰할수 있는 정보 공유 모델☆

Trusted Information Sharing Model in Collaborative Systems

홍승필* 김재현**
Seng-phil Hong Jaehyoun Kim

요 약

빠르게 변화하는 e-비즈니스 환경 내 구성(원)들은 다양한 기술을 통하여 웹 환경 내 협업에 필요 한 효과적인 비즈니스 정보의 공유, 전송, 분배의 필요성이 점점 증가하고 있다. 하지만, 신뢰할 수 있는 비즈니스 환경 측면에서 정보보호에 대한 위험은 항상 존재 하고 있다. 본 논문에서는 "e-marketplace"라는 비즈니스 환경 내 안전하고, 효과적인 접근제어 모델을 제안하였다. 이 제안 된 모델은 분산 환경 내 다양한 비즈니스 객체들간의 안전한 접근제어 정책 수립 및 제어 방안을 기술하였다. 또한 정형화 된 접근제어 모델이 실제 비즈니스 환경 내 용이하게 사용 할 수 있도록 아키텍처와 가이드라인을 소개하였다.

Abstract

Inthe rapidly changing e-business environment, organizations need to share information, process business transactions, and enhance collaborations with relevant entities by taking advantage of the various technologies. However, there are always the security issues that need to be handled in order for the e-business operations to be run efficiently. In this research, we suggest the new security authorization model for safety flexible supporting the needs of e-business (e-marketplace) in an organization. This proposed model provides the scalable of access control policy among multi-domains, and preservation of flexible authorization management in distributed system environments. For servers to take the access control policy and enforcement decisions, we also describe the feasible authorization architecture is concerned with how they might seek advice and guideline from formal access control model.

☞ Keyword : Authorization, Authentication, Access Control, Security Policy, PKI, PMI, e-business

1. INTRODUCTION

The emergence of an e-marketplace is enabling the Internet economy. e-marketplace is known to be beneficial to both the suppliers and buyers in such that business interactions can be efficiently conducted through information sharing and redefining of business-to-business relationships. Further, e-marketplace has promised many benefits to committed entities, and the interest in business community have aroused due to e-marketplace's potential [1]. This leads to the win-win scenario for both parties of which benefits can be maximized as the majority of business-to-business transactions are predicted to be executed via e-marketplace by the year2003 [2]. The impact of Internet on business-to-business (BtoB) commercial operations is growing, and this proliferation of e-marketplace is too important to be ignored. e-marketplace is not an option for the firms to choose in the digital economy. As the companies are fiercely competing for survival, they have to embrace e-marketplace by implementing the stable and appropriate information

* 종신회원 : 성신여자대학교 미디어정보학부
philhong@sungshin..ac.kr(제1저자)
** 종신회원 : 성균관대학교 컴퓨터교육과 조교수
jhkim@comedu.skku.ac.kr(교신저자)

[2006/06/26 투고 - 2006/07/10 심사 - 2006/10/17 심사완료]
☆ 본 연구는 성신여자대학교 학술연구조성비 지원에 의하여 수행하였습니다.

technology (IT) infrastructure as the firms prepares to enter the new business era.

Security is also one of the primary interests of the managers in an organization, especially in the digital business environment where the businesses heavily depend on information flow. Since the web is the center playground of electronic commerce with its far-reaching connectivity, flexibility, and 24 hour availability [2]. The purposes of this research are to identify the access control issues in the value chain of e-marketplace and provide relevant recommendations to resolve the problems using flexible access control policies. We also proposed to authorization model and architecture for distributed environment, especially e-procurement, then support to our feasible approach using case studying with theoretical proven.

This paper consists of seventh chapters. Chapter 1 discusses a brief introduction of this paper. We examine the e-marketplace, and we also conduct the relevant literature review, analyzing the topics of interest in chapter 2. In chapter 3, we explain to briefly related research works and technologies. In chapter 4, we suggest the problem statements based on the analysis of the value chain in e-marketplace with respect to reliable and flexible authorization management, and weakness control/integration. In chapter 5, we introduce and describe new authorization model, then we propose the authorization architecture for feasible approach. In chapter 6, we describe the features and/or benefits of our secure information sharing model using practically in case studying. Lastly, we conclude and future work in chapter 7.

2. BACKGROUND

2.1 e-marketplace

It is clear that the Internet is rapidly changing the ways the business is being conducted. The Internet provides a connected IT infrastructure in which data and information can be efficiently exchanged while firms conduct their business anywhere and anytime at the speed of light. The revolution of e-business is reaching a new phase of business innovation, and it is expected that the BtoB electronic commerce will be a major driving force in the online market. The business transaction volume in BtoB market is exploding with a rapid growth and it far exceeds the volume of business transaction in BtoC market.

Currently, the focal point of e-business is shifting to B2B market and more specifically to e-marketplace where many suppliers and purchasers participate in business exchanges. Therefore, e-marketplace plays an important role in online and networked business environment. The definition of e-marketplace varies with different perspectives.

E-marketplace is a key activity in the value chain of an organization, and many firms are utilizing the information technologies including the Internet to efficiently support the business operations [2]. But, some researchers [3, 4, 5] argue that most of the e-marketplace activities are executed manually with limited technological support. They argue that current system needs an improvement at most organizations and in order to be competitive, the firms have to strategically use the information technologies to enhance its e-marketplace operations. Many companies understand the importance of improving the quality and efficiency of the e-business relationship, knowing that it is the critical factor for their business success (see Fig. 1). This fig. 1 illustrates its broad definition from the B2B stand point of view.

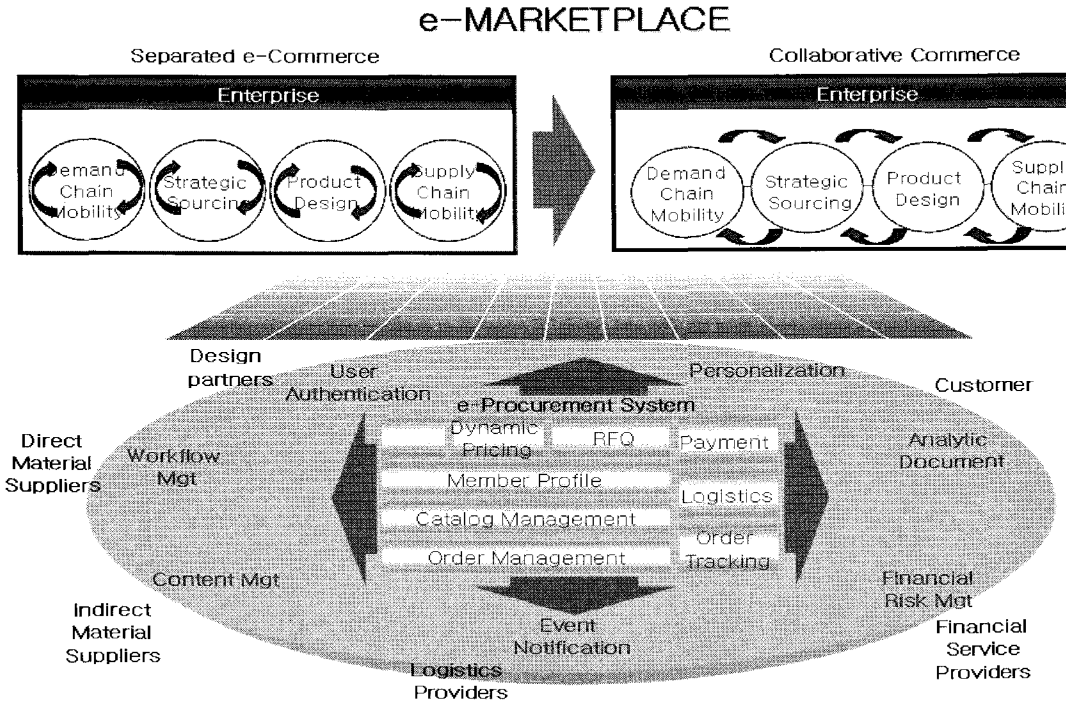


Fig. 1. The definition of e-marketplace

The importance of e-marketplace is being emphasized more recently as the business market is growing in the global scale and the business model of an organization is changing to the extended enterprise model in order to efficiently support the procurement and sales functions [6]. And, knowing that the improvement of production and sales is reaching its limitation in current organizational management structure, it became necessary to adopt the innovative information technologies to provide better support for business operations in e-marketplace.

2.2 Security issues in e-Marketplace

With the introduction of e-business modeling, we have witnessed critical security concerns that need to be studied and analyzed to investigate relevant countermeasures. Our study indicated that some of security issues are still raising inevitable business problems as follows:

Weak Authorization Management System: A user authorization service is composed of variety of nodes and links from many different vendors. There may be dozens of different application systems, and servers. Thus the system manager or operator could be considering the trust authorization management systems for reliable business approach system.

Unobservability: This refers to the inability to observe (or track) while a user is accessing a service. The multi-purpose user can be used to abuse critical information such as payment information without authorized such as permission or legitimate access when the user is used for other services. However, it may be useful to observe activities of the user under certain circumstances such as disaster or medical emergency.

Leakage of Multiple points of control: To reconnect to their business site, users are often required to present their identifications. This can be used to track how often a user reconnect to site, what they shared information systems, even though it is important only to know that the bearer deserves access to the facility. It needs to ensure that a legitimate user/group accesses the associated their own information without any leakage it.

Data management: Collected and managed data and information can be often misused with malicious intent or by mistakes. It is essential to minimize the risk in using the information wrongfully, especially in distributed environments, prohibiting from using business related to information without right permission.

In the subsequent sections, we attempt to articulate possible solutions for key issues involved with the above security concerns.

3. RELATED WORKS

3.1 Related Paper

Hagstrom [7] is proposed to how to development with specific requirements for the access control in workflow system using case study. They represent in Embedded Workflow Service (EWS) data model, and suggest to access modes in EWS. It is emphasized on the problem of work assignment, lockups and delegation. And show to solving problems. For the work assignment issues, they specified access modes and rules for inheritance of these. In lockups, they added specific process document folder and lockup analysis. The delegation problem was addressed by adding delegation relationship to database. However, it still difficult to implement to delegation case such as delegation chains, or loops, and it could not satisfactory way in the applied to real large-scale systems, because of only focus on theoretical approaches.

Hayton [8] describes architecture for open distributed environment using Role Membership Certificate (RMC) for its subsequent use with that service. The first part of this paper shows how a service may define a set of proof rules that specify who may use it and in what way. In this time, delegation issues introduced within proven rules, but it could be insufficient approaches for adapted to real distributed systems even it reflects to case studying, because it only focus on narrow aspects of access policies. The second part of this paper presents the design details of the system. Associated with each RMC issued by service, the service keeps a Credential Record (CR) for revocation handling, but it still need to more specific process or mechanisms for implement for software engineering or developers, because it only explains to logical views of validation of the delegation and revocation.

Chang[9] suggests to the ticket-based delegation service for multiple domain models. This proposed model supports the protection of the high-level resources in various domains using CORBA based security. The secure delegation service that proposed the preservation of the security policies of the underlying resources which support to public-key cryptosystem based ticket between the kerberized domains and the Non-kerberized domain. But it did not mention the specific or general security policies for delegation service in the distributed environments, it also insufficient analysis of multiple domain properties for distributed authorization service for collaboration.

Pearlman[10] approach allows resource providers to delegate some of the authority for maintain fine-grant access control policies, which define a set of individuals, and/or institutions properties by sharing rule form, what has been called a virtual community or Virtual Organization (VO), to communities. It emphasized on how to specify and enforce community policies into multi-institution. But it is not enough explains how to construct the authorization architecture, and policy hierarchy between multi-institutions.

John [11] argues that security design for open distributed processing would benefit from a shift of focus from the infrastructure to individual servers as the owners and enforces of security policy. This paper is also mentioned to how a server-based view could be designed, and implemented from higher authority which maintain their own security policies, and declared access rights to clients, including delegating rights. This paper suggests to the basic security protocol for cascaded authentication, and delegation. But it is not clearly sufficient to explain how well communicated with multi-domain environments which consists of different security policies, and how well designed and implemented to security policies which defined to offer, trade, supply and consume services into large scale environments.

Yialelis [12] describes an overview of an access control model, which is based on the notion of domains to specify access control policies for groups of subjects or targets. The concept of domain is indicated the possibility of partition responsibility or reflection of user specification compare to general groups, and this paper describes the authorization policies provide the access control permission and constraints to limit their applicability. But it did not specific describes too much how to define and analysis the multi-domain policies and how represent to organizational policies and the assignment / revocation to each related to object properties.

3.2 Related Technologies

3.2.1 Role Based Access Control

RBAC has recently received considerable attention as a promising alternative to traditional Discretionary and Mandatory Access Controls (see, for example, [13, 14, 15, 16]). As MAC is used in the classical defense arena, the policy of access is based on the classification of objects such as top-secret level. The main idea of DAC is that the owner of an object has discretionary authority over who else can access that object. But RBAC policy is based on the roles of the subjects and can specify security policy in a way that maps to an organization's structure. A user can be a member of many roles and a role can have many users. Similarly, a role can have much permission and the permissions can be assigned to many roles. Each session relates one user to possibly many roles. Intuitively, a user establishes a session during which the user activates some subset of roles that he or she is a member of. The permissions available to the users are the union of permissions from all roles activates in that session.

3.2.2 Public Key Certificate and Digital Signature

A public-key certificate is digitally signed by a certificate authority (a person or entity) to confirm that the identity or other information in the certificate belongs to the holder (subject) of the corresponding private key. If a message-sender wishes to use public-key technology for encrypting a message for a recipient, the sender needs a copy of the public key of the recipient. On the other hand, when a party wishes to verify a digital signature generated by another party, the verifying party needs a copy of the signing party's public key. Both the encrypting message-sender and the digital signature-verifier use the public keys of other parties. Confidentiality, which keeps the value of a public key secret, is not important to the service. However, integrity is critical, as it assures public-key users that the public key used is the correct one for the other party. ITU (International Telecommunication Union) and ISO (International Organization for Standardization) published the X.509 standard [17], which has been adopted by IETF (International Engineering Task Force). X.509 is the most widely used data format for public-key certificates today and is based on the use of designated certificate authorities (CAs), which verify that the entity is the holder of a certain public-key by signing public-key certificates.

3.2.3 Privilege Management Infrastructure

A PMI (Privilege Management Infrastructure) is to authorization what a PKI is to authentication. Consequently, there are many similar concepts in PKIs and PMIs. While public key certificates are used to maintain a strong binding between a user's name and his or her public key, an Attribute Certificate (AC) maintains a strong binding between a user's names and on or more privilege attributes [18]. Typically, in traditional systems, the access rights are held as Access Control Lists (ACLs) within each target resource. In an X.509 PMI, the access rights are held within the privilege attributes of ACs that are issued to users. Each privilege attribute within an AC will describe one or more of the user's access rights. A target resource will then read a user's AC to see if he or she is allowed to perform the action that is being requested.

4. PROBLEM STATEMENT

In sourcing, manufacturing, and delivering business domains, firms interact with many business partners for information sharing, communication, and business transactions. The business relationships are complicated, characterized as multi-networking. The scope of interactions often goes beyond the boundaries of business domains. Simply, there are many interactions that cross the business domains, and involving many entities in resolving the business issues.

The major problem of current access control view is that it is distributed across many heterogeneous components controlled by the different interacting organizations. As a result of business analysis in above core issue areas, there are many insufficient points in the viewpoints of authorization e-marketplace requirements such as reliability, and scalability. In the business domains which include in Source, Make, and Delivery needs to improve the process efficiency of integration of planning / execution, e-procurement planning / scheme, purchasing / material responsiveness, production / process control, and demand fulfillment. Problem issues in each improvement area are described in table 1. The problem issues need to be addressed with proper actions to improve the authorization management in e-marketplace and enhance the business relationships with the core business partners.

Table1. Access control issues in e-SCM

Process		Subject	Action	Related Information	Access control issues
S	P	S, M	Supply plan, Order plan	- Forecasting, Market information - Order plan - Supply plan.	- Ownership, and access control when Share the Forecasting and market information - Only manufacturer can access for the order information - Only supplier can access for the supply planning information
	E	S, M	Supply, Order	- Ordering. - Type, price, etc. - Stock count	- Insufficient to control for separation of duty, and least of privileges. - Only supplier can access for the stock count information
M	P	M	Production plan	- Production plan, - Additional order plan	- Only authorized manufacturer can read / write production information - Only manufacture can access for the all production related information
	E	M	Production	- Output rate - Inferior rate	- Only authorized manufacturer can update their own production information - Unauthorized could not read / write /update other product information
D	P	M D	Delivery plan, Additional order plan	- Forecasting, Market information - Delivery plan - Storehouse routing - Additional order Plan	- Share Forecasting and market information - Only deliver can access for the Storehouse routing and delivery planning information - Only manufacturer can access for the additional order planning information
	E	M D	Delivery Additional order, Pay	- Delivery status - Delivery confirm - Additional order - Payment	- Share the delivery status and additional ordering information - Only deliver can access for the delivery confirm information - Only manufacturer can access for the payment information

S : Source, M : Make, D : Delivery, P : Plan, E : Execute

5. Secure Information Sharing model

For solving the above problem statements, we are provided to new secure information sharing model, which is called "SAA -Secure Authorization Architecture for e-marketplace" The SAA models that allow reliable authorization management for multi-domain environments where interactions among heterogeneous policy domains are intensive. With the growth of e-commerce applications, access models and mechanisms should facilitate dynamic changes in the content and context of information, allow monitoring of state of the system, and facilitate carrying out transactional activities.

We suggest the SAA models for the interpretabilities among the two or more systems. A user belongs to the some local system can also belongs to another system and such systems are managed respectively, communicate each other when need.

In a local system, a user's access is controlled by it sown roles / rules and access control policy is narrow focus on each properties. If the interoperation is needed between the different systems, a user must be assigned to their position in each system by its access control policy. In this case, a user must login to each system respectively and executes some needed operations. In the viewpoint of this distributed system, it is hard to administrate the policy for not all users in local system but also collaborative systems. The following Fig. 3 represents to new secure information sharing model for e-marketplace.

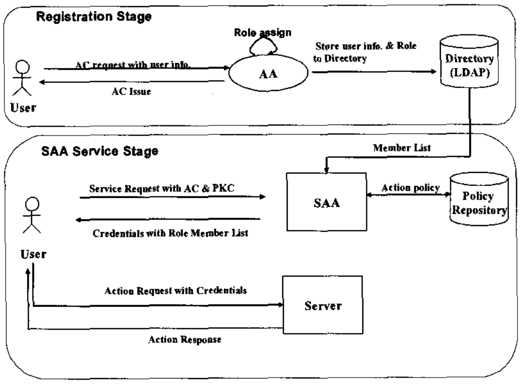

Registration Stage
Role assign
Store user info. & Role to Directory
AC request with user info.
AA
Directory (LDAP)
AC Issue
User
SAA Service Stage
Member List
Service Request with AC & PKC
SAA
Action policy
Policy Repository
Credentials with Role Member List
User
Action Request with Credentials
Server
Action Response

Fig.3. Secure Information Sharing Model

All subjects' attribute certificates are also issued in registration stage and their role and id are stored in the member list directory. Action policy assigned by SAA Manager is based on the subject's information and only SAA manager or administrator controls the PB mechanism for integrity.

5.1 SAA Algorithm

Here is simple algorithm in SAA

```
1 System A request information with an input call to SAA
  1.1 Make an input call using XSL sheets or SXML
  1.2 Establish a SSL connection with SAA
2 SAA check the information which request from System A
  2.1 Check the validation of the System A's public key certificate using PKI
  2.2 Verify the signature in a input call using the A's public key certificate
  2.3 Check the validation of the System A's Attribute Certificate using PMI
  2.4 IF the check is well done, go to next step.
  ELSE send back to error message to System A, and go to Step 5
3 SAA retrieves privileges granted to corresponding the subject's action from policy repository.
  3.1 Retrieves privileges granted to corresponding the subject's action,
  3.2 Assign a reasonable policy which corresponding to a set of subject's information.
  3.3 Policy enforcement checks the policy type.
  3.4 IF the check is well done, go to next step.
  ELSE send back to error message to System A, and go to Step 5
4 SAA sends an output call for each target system B.
  4.1 Generates an output call using XSL sheets or SXML.
  4.2 Establishes a SSL connection and sends an output call to each target system.
SAA mechanism always keeps monitoring the Accept/Drop logs for prevention or detection security accidents.
```

The notations are used in SAA architecture, which describes in logical flow as follows:

SA(m) : Signature generation for input data m by A's private key

U : A subject who requests an actionto be executed in servers

S : A set of all servers that responses to the action requests from U, where Si $\in$ *S, i* $\in$ *{1,⋯, n}*

AM : SAA
SS : a set of all subjects, where U, Si, AM $\in$ *SS*
Let A $\in$ *SS*
IDA : ID of a subject A
Ti : Timestamp,
Ni : Nonce
SigA : Signature of A
TMI : Time interval that the credential is valid
PcertA : Public key certificate of A
ACertA : Attribute certificate of A
TA (Target) : A role or system IDs that are requested to execute some actions from U
TSL : Target system list. If the target of the action in input call is a role, TSL will be a list of addresses and IDs of all member of the Role, otherwise, TSL will contains an address of a target system
Act : Action that U requests to be executed in Si
ActWithP : Action policy
ResPi : Results of the action that is executed in Si
SEK(m) : Symmetric key encryption for input data m by using symmetric key K

Fig. 4 shows the secure authorization architecture for e-marketplace. All subjects establish a SSL session before they communicate with each other for confidentiality. Let SSL connection between U and SAA establish a session key *K1* and SSL connection between U and each server Si establish a session key *K2*.

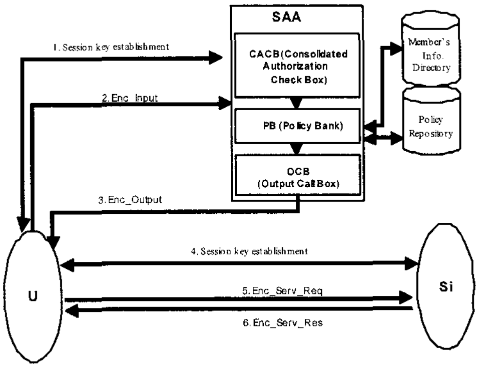


Fig. 4. SAA(Secure Authorization Architecture)

i. Input call

Input call is an service request to SAA, To take a credential for executing actions in System Si, User U generates Input call

Input call := <ID_{AM} *, TA, T1, N1, Act, SigU, PCertU, AcertU >*

SigU = $S_A(ID_{AM}, TA, T1, N1, Act)$

By SSL connection, Input call is encrypted by the shared key K1 and Enc_Input := <SE_{K1}(Input call)> sent to SAA.

ii. Ouput call

Output call is a response of SAA with credential. SAA generates Input call

Output call := < Cred, TSL, T2>

Cred := {IDU , N2, ActWithP, TMI, SigAM}

SigAM = SAA(ID_U*, N2, ActWithP, TMI)*

By SSL connection, Output call is encrypted by the shared key K1 and Enc_Output := <SE_{K1}(Output call)> sent to U.

iii. Serv_Req

Serv_Req is an service request to Si containing credential. U generates Serv_Req

Serv_Req := < ID_{Si} *, T3, SigU, Cred, PcertU>*

SigU = $S_A(ID_{Si}, T3, Cred)$

By SSL connection, Serv_Res is encrypted by the shared key K2 and Enc_Serv_Req := <SE_{K2}(Serv_Req)> sent to Si.

iv. Serv_Res

Serv_Res is a response of Si containing results of the action executed in Si. U generates Serv_Res

Serv_Res := < ID_{Si} *, T4, ResPi, SigSi >*

SigSi = $S_{Si}(IDSi, T4, ResPi)$

By SSL connection, Serv_Res is encrypted by the shared key K2 and Enc_Serv_*Res := <SEK2(Serv_Res)>* sent to U.

5.2 SAA Mechanism

5.2.1 CACB (Consolidated Authentication Check Box)

CACB is a module for maintains the confidentiality of the subjects concerned with SAA. It is possible to have a own special consolidated authentication process, but it is recommended to interconnect with a public authentication organization which is X.509 certificate-and PMI for confidentiality, and extensibility. Generally, computer systems require an additional control to limit the actions or operations that a legitimate subject performs after authentication check is successful, so-called consolidated authentication and authorization. Most e-commerce systems use password-based authentication over the SSL connection. X.509 certificate-based authentication can be used as well, and while public key certificates are used to maintain a strong binding between a user's name and his or her public key, an attribute certificate (AC) maintains a strong binding between a user's names and on or more privilege attributes using PMI. Our approach combines authentication and authorization in a single unit and makes use of X.509 certificate and PMI to carry users' information as shown in Fig. 3. It could be reducing the complexity of management which should be considering user's authentication and authorization information for user reliability, and system scalability.

5.2.2 PB (Policy Bank)

PB is the set of access control policies for passing a system's requests to another system between multi domains. The SAA defined the police framework consisting of policy for interface gathering when enters the policy bank, repositories for storing policy, then policy enforcement for handling in policy decisions. Here is the structure of PB description. We have to check to user verification and validation before entering the PB. The policy gathering is recognized that it can equally be applied or assigned the access control policy that has already defined which services or resources a subject (management, agent, user, or role) can access into different service domains. In our case, it could be possible to suppler want to some business information to manufactures. Then the policy repository is storage that is used for policy decisions, and PB repository has following components in their DB. In this time, policy management should guarantees that each request supports to right access constraints or access control protocol, and updating/revocation in policy status. The policy enforcement triggers to retrieve policy from policy repository check to policy conflict, and evaluated the policy when policy executed from repository.

5.2.3 OCB (Output Call Box)

The OCB (Output Call box) get policy enforcement information from PB, and then OCB generates HTML document using commercial off-the-shelf technologies such as XSL sheets or SXML documents. In this time, each session establishes in SSL connection for secure channel, and The OCB also remains in logging each session for detection / prevention control in later.

6. CASE STUDY

We could defined and analysis the problems or issues in e-marketplace using practically in business scenarios.

Table 2. Policy repository component

Attribute	Meaning
Request Response Check Verifica-tion Order Cancel Pay/Debt	Action is the form of sets in performed between domains, for applying different business operations as following this. - request to information of products or goods - response to information of products or goods - check to products/goods for verification business condition - response to the check action request - order to products/goods which it have already check/verified - cancel products/goods which it have already finished pre-order. - pay /debt to products/goods.
Subject	The human or manager who applies for an action.
Object	The human or manager who executes an action requested by Subject.
Domain	Grouping subjects or objects such as file system directories. In e-marketplace, we are assumed to business domain, whichis consists of three domains: Supplier, Manufacture, and Delivery.
Policy Type	Policies are rules governing the choices in behavior of a system, and policy types are assigned to specific types of the access control policies, which depend on what activities are subject can perform of a set of target objects. In this paper, we are defined to following policy types. Policy_Type_A/A' : A set of subjects must do / not do a set of target objects. Policy_Type_B : A set of subjects must check to do the conflict access control policies to a set of target objects. Policy_Type_C/C' : An actions are permitted / forbidden from set of subjects or a set of target objects Policy_Type_D : An actions are delegatedor obligated from set of subjects or a set of target objects Policy_Type_A : allow action to all subjects. Policy_Type_B : allow action only to the subject to whom the AC was originally granted. Policy_Type_C : allow action only if all subjects in a chain of delegation are authentic. Policy_Type_D : allow action only if the final subject in a chain of delegation is authentic, regardless of the authenticity of any other subjects. Policy_Type_E : allow action only if subjects in a chain of delegation are from some pre-defined set of the security group. Policy_Type_F : allow action only if subjects in a chain of delegation are from some pre-defined, where this set could include clients from other security group.
Priority	The importance of the Subject, information or actions to be performed. It would be representing to Low, Medium, High.

Company A's goals are (1) to develop the collaboration system based on e-business infrastructure with the suppliers and customers at the core contact/access point and (2) to develop IT infrastructure that support e-business transformation of core business processes (integration, optimization, forward visibility) with minimum security issues. Fig. 5 represents to the framework of e-business in company A. Through the collaboration with suppliers and customers, company "A" focuses on enhancing the business efficiency in procurement, purchasing, production, product development, sales, and customer service

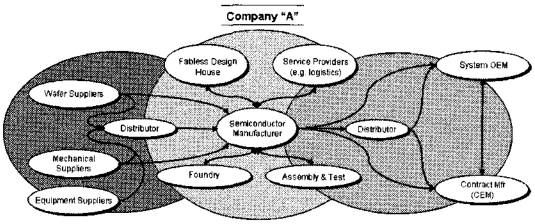


Fig. 5. Front · Back-end e-Business Process of Company A

The following example describes to the SAA algorithm in "company A" case.

```
1. System U requests the number of remain products and
      price of them to all registered Suppliers in SAA.
   Input call:= <IDAM , TA, T1, N1, Act, SigU,
   PCertU,AcertU >
      TA : = Supplier
      Act := (REQUEST NumberOfProduct, Price)
2. SAA verify the signature SigU by using PcertU.
3. If PCertU is valid, Authorization Unit check the
   validationof the ACertU by using AA's public key
   certificate.
4. If ACertU is valid, retrieve a domain
   information,Manufacturer, from A's AcertU.
5. PB executes the policy gathering from the
   Manufacturer domain table in policy repository and the
   policy enforcement.
6. SAA generates output call.
      Output call := < Cred, TSL, T2>
      Cred := {IDU , N2, ActWithP, TMI, SigAM}
   ActWithP := {(REQUEST NumberOfProduct,
   Price),Policy_Type_A, High}
   TSL := {S1, S2, ...., St}, where Si  TSL is a suppler
   registered in supplier domain.
7. SAA sends output call and logging.
```

Systems Si checks the remaining products within its local domain and sends response to System A. The procedure of response is the SAA of request procedure. Then System U can gather the information, the number of product and price, from each response. By suggest the same procedures, order and pay can executed also through SAA mechanism. The following table 3 describes in the assigned security policy among multi domains in e-business environments.

Table 3. Manufacturer domain table in policy repository

S	A	TA	PT	P	O
System A	REQUEST Number Of Product	Supplier	Policy_Type _A	M	System B
System A	REQUEST Price	Supplier	Policy_Type _B	H	System B
System A	REQUEST Price	Supplier	Policy_Type _C	H	System C

S : Subject, A : Action, TA: Target, PT : Policy Type, P : Priority, O : Object, H : High, M : Middle, L : Low

Based on the realization, we identify specific goals that inform the design of secure information model using SAA mechanism.

Strong Authorization Service: A user wishing to access community resources contacts the SAA server, the system administrator or management to easily to keep track of its membership and secure access control policies, because CACB (Consolidated Authentication Control Box) mechanism can reduce additional overheads that the traditional two-step approach has. Using a signed token, we can provide "dual verification" for e-marketplace users in which a signed token is used to verify users'identity and privileges. It also CACB algorithm investigate more sophisticated way to deploy our approach using commercial off-the-self technology such as privilege management infrastructure (PMI) and attribute certificate. In PB (Policy Bank), it also provide centralized monitoring condition which is handle how well subjects can present at a resource to gain access on behalf of the business community condition. It could be improve ease of use and accuracy of the administration process even if access control is implemented in a variety of heterogeneous components, and the system administration needs to concentrate only on this very unit in which all security related configurations are maintained

Trust Policy Management: The SAA mechanism should rely on a simple mode transaction that covers the different range of large-scale multi-organizational systems. Because SAA mechanism strictly enforces stored access policies that have been already defined in PB repository of SAA. This means that it is very hard to modify/delete our reserved rules or policies by unauthorized people. Additionally, our policies are supposed to reserve a couple of business action (Request/Response/ Check/Verify/Pay/Debt) cases for easily adoptable business logic. There is no change in the policy type without permission or privilege. The changing managements are only aimed at PB into SAA, and it is no rights to do any other operations, so it could be more easily support to centralized management.

Well-defined Security Policy: A user wishing to secure access community resources contacts the SAA server. The system manager can easily keep track of user's business condition and select fine-grained access control policies, because PCB mechanism can verify and validate user's information. In PB, it also provides centralized monitoring condition, which handles how well users can present themselves to gain access on behalf of the business community condition. It could improve ease of use and accuracy of the administration process even if access control is implemented in a variety of heterogeneous components, and the user (Buyer or Seller) or system manager needs to concentrate only on this very unit in which all security related configurations are maintained.

7. CONCLUSION AND FUTURE WORK

In this paper, we have defined access control issues in e-marketplace. To approach the new secure information sharing model to concerns in e-marketplace, we have proposed an innovative approach called "SAA (Secure Authorization Architecture for e-marketplace)". This SAA model proposes to flexible access control into multi-domains, which has different access control policies. And the SAA model is support to the multilevel security that has generated great interest in the business community as strong security modes, and it is also proven to how priority messaging control among different domains. Even though this work is applied to e-commerce environment, we believe that this mechanism can be deployed into large-scale collaborative environments such e-government and workflow systems. Our future work will be focus on controller design for SAA, which can support to cascade delegation status, and flexible to handling in request real time feedback.

REFERENCES

[1] Andrew Lancastre and Luis Filipe Lages, "The relationship between buyer and a B2B e-marketplace: Cooperation determinants in an electronic market", Industrial Marketing Management, Volume 35, Issue 6, Pages 774-789, August 2006.

[2] Laudon, K. C. and Laudon, J. P., "Management Information Systems: Managing the Digital Firm", Pearson Education Inc., Upper Saddle River, NJ, 2006.

[3] Tzong-Ru Lee and Jan-Mou Li, "Key factors in forming an e-marketplace: An empirical analysis", Electronic Commerce Research and Applications, Volume 5, Issue 2, Pages 105-116, Summer 2006.

[4] Ray, G., Muhanna, W. A., and Barney, J. B., "Information Technology and the Performance of the Customer Service Process: A Resource-based Analysis", MIS Quarterly, Vol. 29, Issue 4, pp. 625~651, December 2005.

[5] Nikos Karacapilidis, Alexis Lazanas, George Megalokonomos and Pavlos Moraïtis, "On the development of a web-based system for transportation services", Information Sciences, Volume 176, Issue 13, Pages 1801-1828, July 2006.

[6] Karl Kurbel and Iouri Loutchko, "A model for multi-lateral negotiations on an agent-based job marketplace", Electronic Commerce Research and Applications, Volume 4, Issue 3, Pages 187-203, Autumn 2005.

[7] Hagstrom, A.; Fak, V.; Vandenwauver, M "EWS-a case study on access control in workflow systems". Enabling Technologies: Infrastructure for Collaborative Enterprises, 2000. Proceedings. IEEE 9th International Workshops on 2000, Pages 213 - 218, 2000.

[8] R.J. Hayton, and, K. Moody, "Access Control in an Open Distributed Environment", Security and Privacy, Proceedings IEEE Symposium, Pages 3 -14,1998.

[9] Kyung-Ah Chang; Tae-Seung Lee;Bang-Hun Chun; Tai-Yun Kim, "Ticket-based secure delegation service supporting multiple domain models" , Dependable Computing, 2001. Proceedings. 2001 Pacific Rim International Symposium, Pages 289 - 292, 2001.

[10] Pearlman, L.; Welch, V.; Foster, I.; Kesselman, C.; Tuecke, S., "A community authorization service for group collaboration" Policies for Distributed Systems and Networks, 2002. Proceedings Third International Workshop on 2002, Pages 50 - 59, 2002.

[11] John A Bull, L Gong, K Sollins, "Towards Security in an Open Systems Federation", Proceedings ESORICS 92, Springer LNCS, Pages 3- 20, 1992.

[12] Yialelis, N.; Lupu, E.; Sloman, M, "Role-based security for distributed object systems", Enabling Technologies: Infrastructure for Collaborative Enterprises, Proceedings of the 5th Workshop, Pages 80 - 85, 1996.

[13] William Tolone, G.J. Ahn, Seng-Phil Hong,and Tanusree Pai, "Access Control in Collaborative Systems" ACM Computing Surveys, Vol. 37, No. 1, ACM, March, 2005.

[14] A. T. Group, "Cryptographic protection of scada communications general recommendations." Draft3, AGA Report No.12 by American Gas Association, August, 2004.

[15] Ninghui Li, and Mahesh V. Tripunitara, "Security Analysis in Role-Based Access Control", SACMAT'04,June2-4, Yorktown Heights, New York, USA, Pages 126-135, 2004.

[16] Ravi Sandhu and Venkata Bhamidipati, "The ARBAC97 Model for Role-Based Administration of Roles", Preliminary Description and Outline Proceedings of

second ACM workshop on Role-Based Access Control, November, 1997.

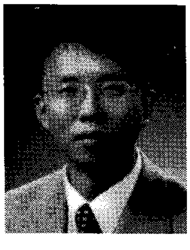
[17] Subhashini Raghunathan, Armin R. Mikler and Cliff Cozzolino, "Secure agent computation: X.509 Proxy Certificates in a multi-lingual agent framework", Journal of Systems and Software, Volume 75, Issues 1-2, Pages 125-137,15 February 2005.

[18] Bernd Blobel, Ragnar Nordberg, John Mike Davis and Peter Pharow, "Modelling privilege management and access control", International Journal of Medical Informatics, Volume 75, Issue 8, Pages 597-623, August 2006.

◐ 저자소개 ◑

홍승필 (Seng-phil Hong)

1993년 Indiana State University (학사)
1994년 Ball State University (석사)
1997년 Illinois Institute of Technology (박사수료)
2002년 한국정보통신대학교 (박사)
1997년 ~ 2004년 LG CNS Systems, Inc.
2005년 ~ 현재 성신여자대학교 미디어정보학부
관심분야: 접근제어, 통합인증, 정보보호 아키텍처, 유비쿼터스 보안, 프라이버시 보호
E-mail : philhong@sungshin..ac.kr



김재현 (Jaehyoun Kim)

1988년 성균관대학교 수학과 졸업(학사)
1992년 Western Illinois University 대학원 전산학과 졸업(석사)
2000년 Illinois Institute of Technology 대학원 전산학과 졸업(박사)
2001년 ~ 2002년 국민은행(구 주택은행) CTO
2002년 ~ 현재 성균관대학교 컴퓨터교육과 조교수
관심분야 : 객체지향 소프트웨어공학, 컴포넌트 기반 개발(CBD), etc.
E-mail: jhkim@comedu.skku.ac.kr