ISSN 1598-9798

데이타베이스연구

28권 제1호 2012년 4월

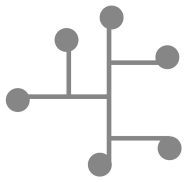
분산 EPCIS 환경에서 RFID 비즈니스 데이터의 접근 메커니즘

Secure RFID Business Data Access Mechanism in Distributed EPCISs

박영욱, 류우석, 우문언, 권준호, 홍봉희
Yong-Xu Piao, Woo-Seok Ryu, Wen-Yan Yu, Joon-Ho Kwon, Bong-Hee Hong

데이터베이스 소사이어티
Database Society

사단법인 한국정보과학회
The Korean Institute of Information Scientists and Engineers



분산 EPCIS 환경에서 RFID 비즈니스 데이터의 접근 메커니즘

Secure RFID Business Data Access Mechanism in Distributed EPCISs

박영욱(Yong-Xu Piao)[1], 류우석(Woo-Seok Ryu)[2], 우문언(Wen-Yan Yu)[3], 권준호(Joon-Ho Kwon)[4], 홍봉희(Bong-Hee Hong)[5]

요 약

RFID 기술은 최근 들어 물류, 군사, 의료 등 많은 응용 분야에서 활용되고 있다. RFID 태그의 위치 추적은 RFID 응용의기본적인 요구사항이다. EPCIS는 RFID 시스템에서 태그 이벤트를 저장하는 정보 저장소이다. RFID 태그의이동 정보는 해당 태그의이동 경로에 따라 여러 분산된 EPCIS에 저장되므로, 태그의추적을 위해서는 서로 다른 소속기관에 의해 관리되는 복수의EPCIS 시스템에 접근하는 것이 필요하다. EPCIS 별로 서로 다른 접근 제어 방식을 가지고 있게 되면 사용자가 개별 EPCIS 각각에 대해 인증 및 인가정보를 유지해야 하는 문제가 발생한다. 본 논문에서는 분산 EPCIS 환경에서 안전한접근 제어를 위한 접근-키 기반의 접근 제어 메커니즘을 제안한다. 제안하는 메커니즘에서 접근-키는 사용자의 인증 및 사용자 등록정보를 포함함으로써, 다른 EPCIS에서 접근-키를 기반으로 사용자를 인증하고 접근 권한을결정할 수 있도록 한다. 이 접근 권한을기반으로 EPCIS는 사용자의 질의를 재설정하여 주어진 권한에 적합한질의 결과를 생성한다. 분산 인증 처리를 통해 접근 제어의 가용성과 함께 처리 성능을 향상시키는 이점이 있다. 실험을 통해 본 논문에서 제안한 접근 제어 메커니즘에 의해 발생하는 EPCIS의 부하가 납득할 만한 수준임을 입증한다.

주제어: 분산 EPCIS, 접근 제어, 접근-키

1 부산대학교 컴퓨터공학과, 박사과정
2 부산대학교 컴퓨터공학과, 박사후 연수연구원
3 중국 InterActive Corp, Program Manager
4 부산대학교 물류IT학과, 교수
5 부산대학교 컴퓨터공학과, 교수, 교신저자
† 이 논문은 부산대학교 자유과제 학술연구비(2년)에 의하여 연구되었음
+ 논문접수: 2012년 2월 1일, 심사완료: 2012년 3월 30일

Abstract

Recently, RFID technology is widely used in logistics, military, health and other application fields. In RFID applications, with RFID tag mobility, RFID data are stored in distributed EPCISs which is RFID data repository component of RFID system. RFID track and trace ability are widespread demand in various applications.Its realization results in cross EPCIS data accessing in multiple organized RFID systems. In this study, we focus on RFID data access control in distributed EPCISs. To realize secure access control for distributed EPCISs access, an access-key based accesscontrol mechanism is proposed; in this mechanism, digitally signed access-key is designed to authenticate user and index user registration information which is necessary for user access right decision. Access-key based access control mechanism enables user to be authenticated by the EPCIS which the user registered in. Additionally, taking use of access-key, accessed EPCIS obtains user registration information for deciding user access right. Based on user access right, EPCIS enforces access control and onlyprovides authorized data to user. Compare with traditional centralized access control, proposed access-key based mechanism enhances availability of access control and it also improves performance of access control processing with distributed authentication process. At last, we check the access control overhead through experiments evaluation. The results of experiments show that the access control brings acceptable overhead.

Keywords: Distributed EPCISs, Access Control, Access-key

1. Introduction

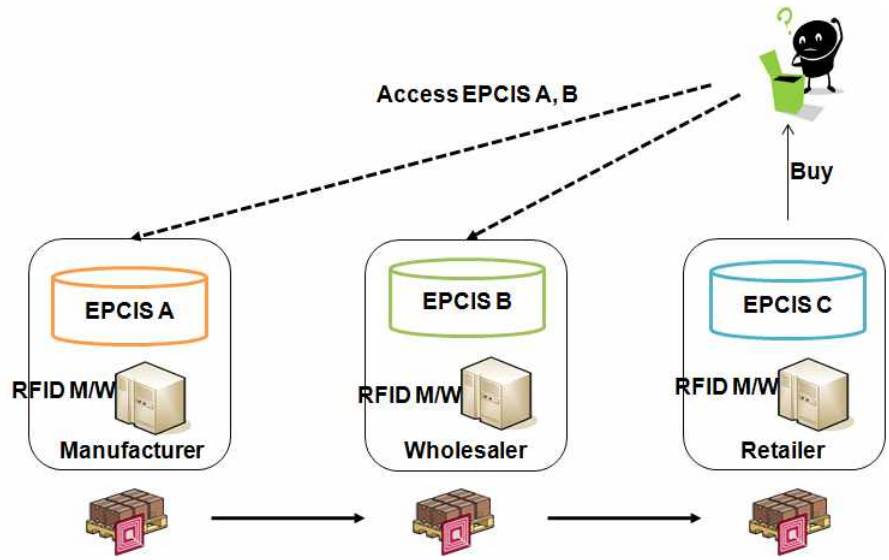
RFID (Radio Frequency IDentification) is a wireless automatic identification technology. It has been widely used in logistics, military, health, vehicle supervision and other fields [1, 2]. In RFID applications, RFID tags are attached to objects which are identified and managed using RFID system. Tagged objects usually travel across multiple sites. Through RFID infrastructure, the RFID data are collected and stored in distributed RFID data repositories which are implemented according to EPCIS (Electronic Product Code Information Services) standard [3].

EPCIS is a global standard which guides implementation of RFID data information services within and across enterprises. EPCIS defines RFID event data meaning and structure. Query interfaces are also designed to provide RFID data services in RFID applications. Based on EPCIS standard, RFID solution should implement query interfaces and RFID data repository for RFID data retrieving and storing. Through EPCIS query interface, anyone can share any RFID data stored in EPCIS implementation (hereafter EPCIS implementation is referred to as EPCIS).

Although RFID data sharing realizes traceability and visibility for RFID applications, it is still constrained by security and privacy requirements. For example, two competitive retailers, they purchase products from the same wholesaler. Both of them can obtain RFID data from wholesaler EPCIS without any limitation. In such a case, one retailer can infer competitive retailer's stock quantity, product category and other critical information from wholesaler RFID data; the retailer will change product price or competitive strategy accordingly. This is not conducive to fair competition between retailers. This example motivates us to study RFID data access control.

Since the mobility of RFID tag, one RFID tag may go through several RFID system sits. At each RFID system sit, RFID tag data are collected and stored in the corresponding EPCIS. As a result, the RFID tag data are stored in distributed EPCISs. When a user wants to trace a specific tag, several EPCISs should be accessed for the tag trajectory information. As shown in Figure 1, user bought a product at retailer. Except for product information in retailer's EPCIS, user may be interested on product information in manufacturer's and wholesaler's EPCISs. Without access control, user is able to retrieve EPCIS A, EPCIS B and EPCIS C respectively. From security perspective, unlimited RFID data access leads to critical information leakage. Each EPCIS access should be under secure access control, only authorized RFID data are returned to the user, i.e. all three EPCISs must be able to authenticate user and decide the appropriate user access right. To implement secure data access in distributed EPCISs, EPCIS access control mechanism should address the following requirements;

Authentication: any EPCIS should be able to



[Figure 1] Distributed EPCISs access scenario

authenticate any valid user. Before data accessing, EPCIS has to determine whether RFID data requestor is a valid user or not.

Authorization:for each legal RFID data request, EPCIS should be able to decide the appropriate user access right. And only authorized data is provided to the user according to user access right.

Many researchers have focused their attentionson RFID data access control. Eberhard and Markus presented policy language for fine-grained EPCIS data access control [4]; the policy language specifies access right by defining EPCIS data type and attributes constraints. However, this study is based onthe known identities or roles. It is impossible to know all visitors for EPCIS since each EPCIS cannot manage all users. Distributed EPCISs data access control is similar with distributed system access control. In distributed system access control studies, most of them focus on access right delegation across organizational boundaries. Many studies address different domain access right delegation through role mapping [5] [6]. Individual site decide user access right using user role information. Since different EPCISs have different RFID data, the same user role has different access right in different EPCISs. Based on the user role in other EPCIS, EPCIS cannot determine which tags are accessible, which RFID data are accessible for the user. User role is not sufficient for EPCIS access right decision. More user registration information is necessary for user access right decision. Few studies try to decide user access right using original user registration information.

Our previous study [7] introduces a concept of access-key based authentication and authorization. Design and implementation are main contributions of the previous work.

However, Access-key based mechanism is not clearly presented for authentication. Authorization approach also has not been considered in detail. Based on access-key concept, we further consider how to authenticate user and authorize access right to user in this study. With enforcing an extended role based access control in EPCIS, we efficiently apply role mapping based authorization in our solution. Firstly, an extended RBAC (Role Based Access Control) [8] [9] model is presented for restricting EPCIS data access. It combines user accessible RFID tags and RFID data constraint to represent user access right. Additionally, we re-consider access-key based EPCIS access mechanism for authentication and authorization in distributed EPCISsaccess. This mechanism achieves distributed EPCISs authentication and authorization with only once EPCIS user registration. Every registered user is assigned to digitally signedaccess-key. For each user request, query with access-key are sent to the accessed EPCIS. Using access-key, the accessed EPCIS is able to authenticate user and index user registration information which is for user access right decision. After user access right decision, EPCIS implements limited data access by rewriting query and filtering query result according to the user access right.

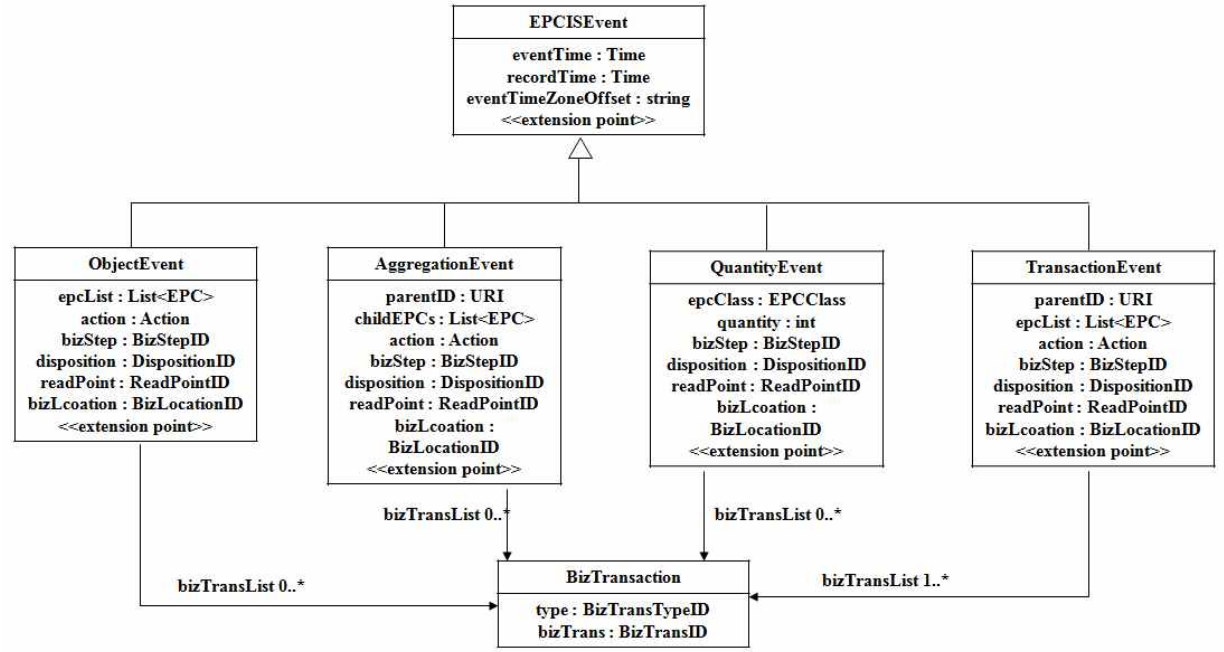
This paper is organized as follows; some related concepts and notion are introduced in section 2. Section 3 presents secure RFID data access in single EPCIS. Proposed access-key based EPCIS access mechanism is explained in section 4. Section 5 gives query processing procedure with access control. Performance experiments result are shown in section 6. At last, we conclude our study in section 7.

2. Preliminaries

2.1 EPCIS

EPCIS is one component of EPCglobal network. It is designed as RFID data repository for EPC-related data services. EPCIS provides standard query interfaces which make RFID data available for all clients and users.

RFID data are stored in EPCIS as four kinds of RFID business event data; ObjectEvent, AggregationEvent, QuantityEvent and TransactionEvent. As shown in Figure 2, EPCISEvent is a base class for all event types. Four kinds of business eventsinherit attributes from EPCISEvent. Each event type has several its own attributes. ObjectEvent represents RFID tag observation information. It records that one or more RFID tags are recognized by RFID system. AggregationEvent describes that oneor more RFID tags have been aggregated to one another object. QuantityEvent presents number information of particular type object. TransactionEvent describes the association or disassociation of RFID tags to one or more business transactions.



[Figure 2] RFID business event in EPCIS

In RFID system, each tag may generate one or more event types. That means the same tag data can be included in different event data. Therefore, RFID event data can be considered as hierarchical archive. Each tag can generate several types' event data. Each event data has several attributes. Access control on RFID event data should follow hierarchical characteristic. Access right firstly should define which tags are accessible, then which event types are accessible and which attributes are accessible.

EPCIS provides data sharing service through query interfaces. Query predicates are defined as a list of query parameters. Each query parameter is a query predicate. Figure 3 shows an EPCIS query example. This EPCIS query defines two query predicates; one predicate is on evnetType; eventType equal to ObjectEvent. The other one is on epc(Electronic Product Code) attribute; epc equal to urn:epc:123.456.693, where epc is RFID tag identification value format. The query result only includes ObjectEvent data which has epc attribute equal to urn:epc:123.456.693.

From security perspective, EPCIS specification introduces some bindings for mutual authentication between EPCIS and client application. Specially, AS2 (Applicability Statement 2) binding achieves security using digital signature and encryption technology. Digital signature data addresses integrity verification and user authentication. Encryption guarantees the confidentiality of data. However, these bindings only address authentication between EPCIS and client. End user authentication is not considered in EPCIS specification. On the other hand, some

```
-<params>
    <param>
        <name>eventType</name>
        <value>ObjectEvent</value>
    </param>
    <param>
        <name>MATCH_epc</name>
        <value>urn:epc:123.456.693</value>
    </param>
</params>
```

[Figure 3] EPCIS query example

non-normative authorization suggestion is appear in EPCIS specification. However, it does not specify how to decide authorization.

2.2 Distributed EPCISs

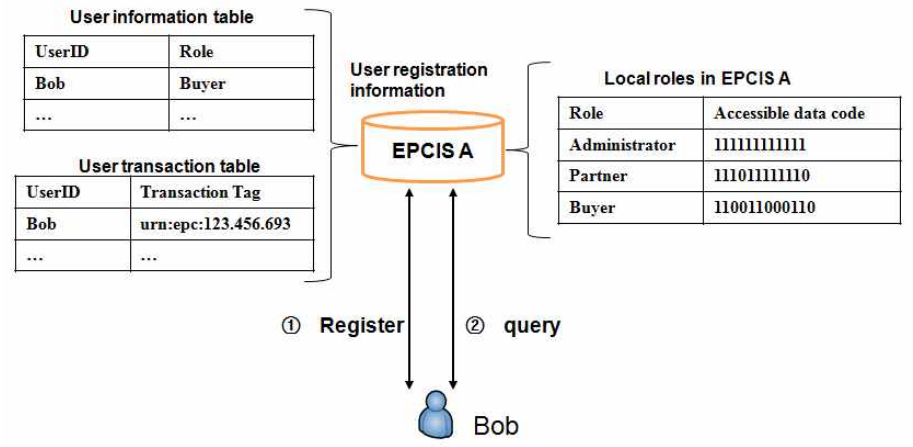
Because of mobility of RFID tag, RFID tags go through multiple RFID systems. Each RFID system has its own EPCIS. Therefore, RFID data are collected in distributed EPCISs. These distributed EPCISs are collaborating to provide information services. User firstly obtains address of EPCIS from discovery services (DS) [10]. All EPCISs share RFID event with users. RFID event data are accessed by user without any limitation. To avoid leakage of critical information in EPCIS, user access should be under access control. Therefore, any EPCIS must authenticate user and know the access right of user.

Main issue of access control enforcement in distributed EPCISs is user authentication and authorization without user registration. It is impossible to require user to enroll in all EPCISs. When EPICS receives a user request, EPCIS firstly authenticates user and enforces access control according to user access right. However, if user did not enroll in the EPCIS, EPCIS cannot directly authenticate user and also does not know user access right. In following section, we present our solution for distributed EPCISs authentication and authorization.

3. Secure RFID data access in single EPCIS

3.1 Registration in single EPCIS

In single EPCIS, user firstly enrolls in one of EPCISs which is called registered EPCIS. Unique user identification (userID) and a role are assigned to registered user. Additionally, user transaction information is stored in registered EPCIS. Transaction information mainly records a set of RFID tags which are accessible for the user. Userinformation and transaction information are stored in registered EPCIS as user registration information. At the same time, a



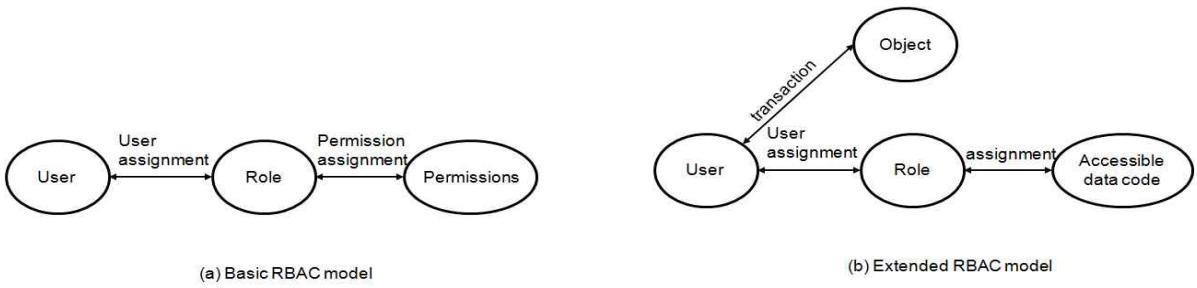
[Figure 4] Secure RFID data access in single EPCIS

digitally signed access-key is assigned to registered user. EPCIS authenticates user by checking signature of access-key. Access-key structure is explained in section 4. Figure 4 shows a user registration procedure. Bob is its userID, role is buyer and transaction tag is urn:epc:123.456.693, i.e. urn:epc:123.456.693 is accessible tag to user. User access right decision is based on the user registration information and EPCIS local policy.

3.2 Extended RBAC for access right decision

In our solution, user access right is decided with accessible tag, user role and EPCIS local policy. Extended RBAC model is suggested to represent EPCIS local policy of user access right decision. RBAC is an approach for restricting user access. Basic RBAC model defines a set of roles, and each role is associated with a set of permissions. Every legitimate user is assigned to one or more roles. Indirectly, user has permissions of role via relationship between role and permissions. Benefits of RBAC model are to reduce duplication access control relationship and improve accuracy of access control. However, basic RBAC model is not suitable for RFID business event data. The reason is that a lot of RFID event data are stored in EPCIS. Accordingly, many users have access right on different RFID event data. Applying basic RBAC has to create a lot of roles for permitted relation between users and RFID event data. For example, 100 tags related RFID event data are stored in EPCIS. 100 users have access right on 100 tags respectively. 100 roles are required to associate 100 users with 100 tags related event data. Too many roles make access right management difficult.

We extend RBAC model by adding object element. Accessible data code is associated with role instead of permissions. Figure 5 shows extended RBAC model. Object element is a setof tags. Association of users and object represents

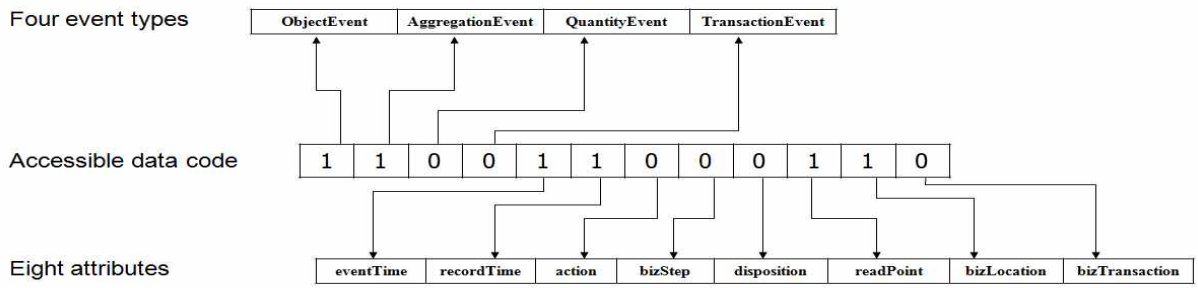


[Figure 5] Extended RBAC model

user and its accessible RFID tags. That means user can access all these tags related RFID event data. Accessible data code specifies accessible event types and accessible attributes for the role. Objectinformation actually denotes accessible RFID event data which are related to the tag set. User role associated accessible data code defines constraints on this event data set. Therefore, object element and access code represent user access right in extended RBAC.

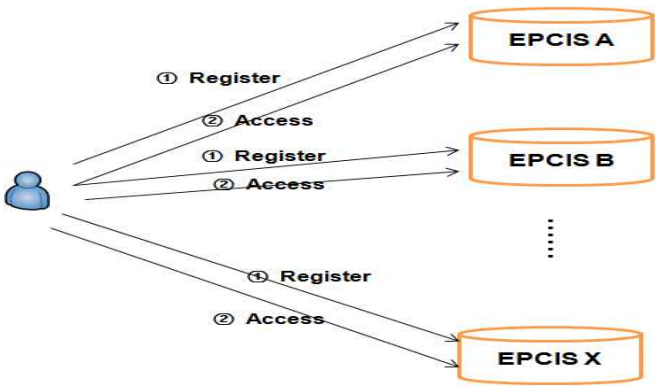
Accessible data code is 12 bits binary code. First 4 bits specify accessible event types; each bit corresponds to one event type. If value is 1, corresponding event type is accessible; else this event type is not accessible. Remaining 8 bits specify accessible attributes. Let's use example to illustrate the accessible data code. As shows in Figure 6, accessible data code is 110011000110. From first 4 bits, we know accessible event types; ObjectEvent and AggregationEvent are accessible; while QuantityEvent and TransactionEvent are not. 8 bits attribute code shows that eventTime, recordTime, readpoint and bizlocation attributes are accessible, and other attributes are not.

As above example shown in Figure 4,when Bob sends request to EPCIS A, Bob has access right on tag urn:epc:123.456.693 which stored in transaction table. Role of Bob is buyer. Buyer role is associated with accessible data code 110011000110. Using accessible tag and accessible data code, Bob' access right is decided.



[Figure 6] Accessible data code example

Bob can access ObjectEvents and AggregationEvents which contain tag



[Figure 7] Naive approach for secure distributed EPCISs access

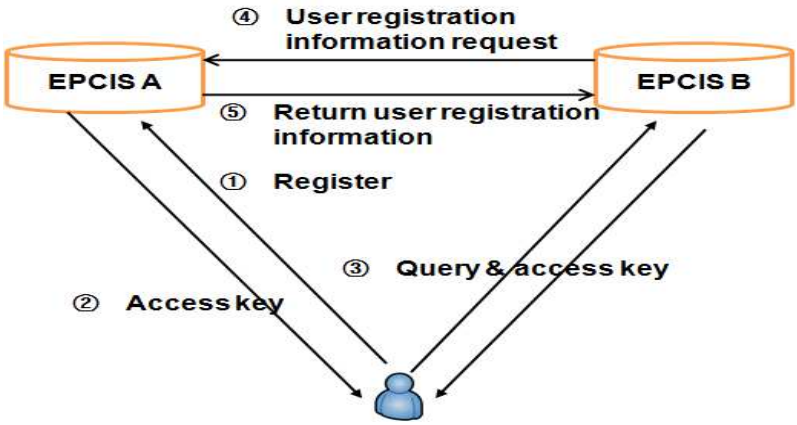
urn:epc:123.456.693. Other typeevent data arenot accessible. Furthermore, the accessible attribute values of ObjectEvent and AggregationEvent are limited by last 8 bits of accessible data code. Authorized ObjectEvent and AggregationEventdata only has recordTime, eventTime, readPoint and bizLocation attributes. Other attributes are limited for Bob.

4. Access-key based access mechanism for distributed EPCISs

4.1 Overview of access-key based access mechanism

In distributed EPCISs, naïve approach for realizing user authentication and authorization is that user enrolls in all accessed EPCISs, i.e. all EPCIS store the user registration information and access right. Naïve approach is shown in Figure 7. Each EPCIS assigns a unique identification to registered user. With multiple registrations, many userIDs are assigned to registered user. It is unacceptable for user to manage too many userIDs. The other problem of this approach is inconsistency of user registration information and access right in different EPCISs. Any user registration information modification leads to update in all EPCISs.

We propose access-key based access mechanism for distributed EPCISs access. For this mechanism, basic assumption is that any two EPCISs trust mutually. Main feature of this mechanism is once user registration for distributed EPCISs access authentication and authorization. Authentication is addressed by user registered EPCIS regardless of which EPCIS is accessed. Registered EPCIS can be considered as an authentication server for the user. Access mechanism process is shown in Figure 8. Digitally signed access-key is designed to address user authentication in distributed EPCISs. Access-key has the registered EPCIS address information. This information enable accessed EPCIS to locate that registered EPCIS. And, accessed EPCIS entrusts registered EPCIS with



[Figure 8] Overview of access-key based EPCIS access mechanism

user authentication. Registered EPCIS also need to send user role and user accessible tags information to accessed EPCIS. Based on registered EPCIS provided information, accessed EPCIS decide user access right. The whole authentication and authorization procedure is described as the following steps;

① Registration: before accessing EPCIS, user must enroll in one EPCIS. User registration information such as userID, user role and transaction information should be stored in this EPCIS. With these user registration information and EPCIS local policy, EPCIS can decide user access right.

② Access-key publication: EPCIS assigns an access-key to every registered user. Access-key is used to authenticate user. And, index information in access-key enable accessed EPCIS to retrieve user registration informationfor user access right decision.

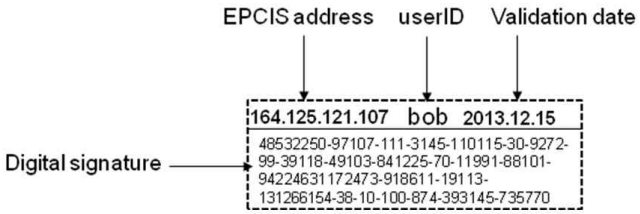
③ User query with access-key: when user issue query to an EPCIS. The access-key should be included in the user request.

④ Authentication request to registered EPCIS: accessed EPCIS can obtain address of registered EPCIS from access-key. Accessed EPCIS sends authentication request and user registration information request to registered EPCIS with an access-key.

⑤ Authentication and Response from registered EPCIS: registered EPCIS verifies user's validity by checking signature of access-key. After user authentication, registered EPCIS returns user accessible tags and user role to user accessed EPCIS.

⑥ Query processing with access right: accessed EPCIS receives user accessible tag and user role information. User access rightis decided based on accessed EPCIS local policy. According to user access right, accessed EPCIS processes user query and returns authorized RFID data to user.

4.2 User registration and access-key publication



[Figure 9] An example of access-key

User registration procedure is same with registration in single EPCIS. User registration information is stored in registered EPCIS. An access-key is assigned to registered user.

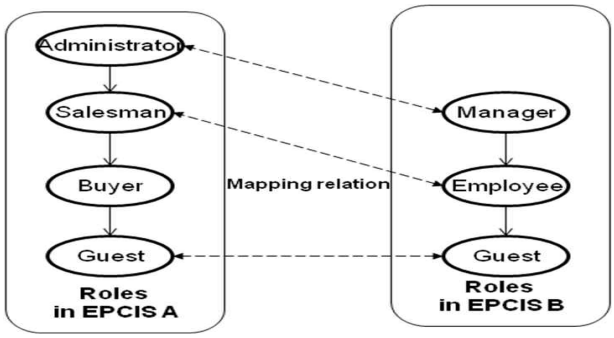
Access-key is a digitally signed data structure which is used to authenticate user and index user registration information. Basically, access-key consists of four fields; registered EPCIS address, userID, validation date and digital signature. Registered EPCIS address and userID are combined as index information to find user registration information. Validation date specifies lifecycle of access-key. Through checking digital signature, registered EPCIS measures the validity of user. At same time, digital signature can protect access-key from modification for guaranteeing the integrity of access-key. Figure 9 shows an access-key example.

4.3 Access-key based authentication

In order to authenticate user, access-key should be included in user query request. Accessed EPCIS can obtain address of registered EPCIS from user access-key. Authentication request and registration information request is sent to registered EPCIS at the same time. Registered EPCIS authenticates user by checking signature of access-key. Since user access-key is published by registered EPCIS, it is able to authenticate the validity of access-key. After user authentication, user accessible tags and user role are returned to EPCIS which user accessed. This information is used to decide the user access right.

4.4 Access right decision across EPCISs

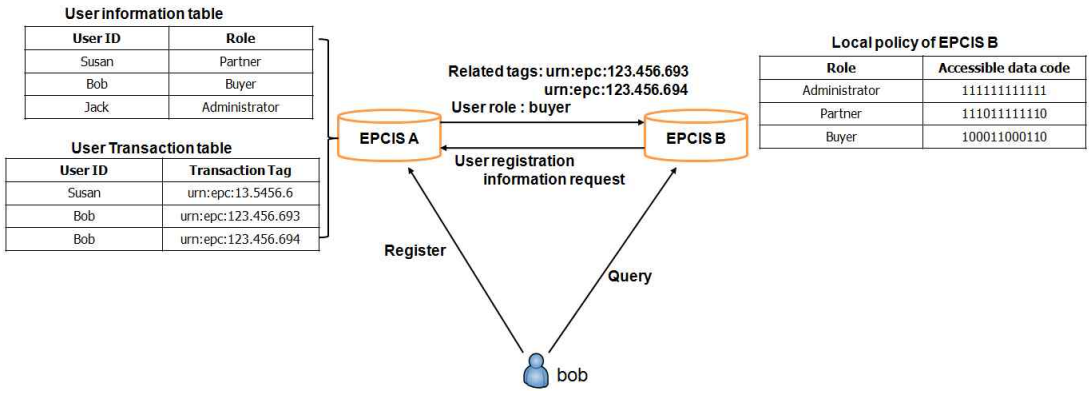
Accessed EPCIS decides user access right based on extended RBAC model. Object and role elements are required for deciding user access right. Accessed EPCIS requests user accessible tags and user role from registered EPCIS. Received accessible tags are object element in extended RBAC model. Problem is user role translation from registered EPCIS to accessed EPCIS. Because of individual EPCIS defines user role set by EPCIS itself, the role names and corresponding accessible data codes are different. Sometimes, accessed EPCIS receives a user role from registered EPCIS, there is no role name is



[Figure 10] Role mapping between EPCIS A and EPCIS B

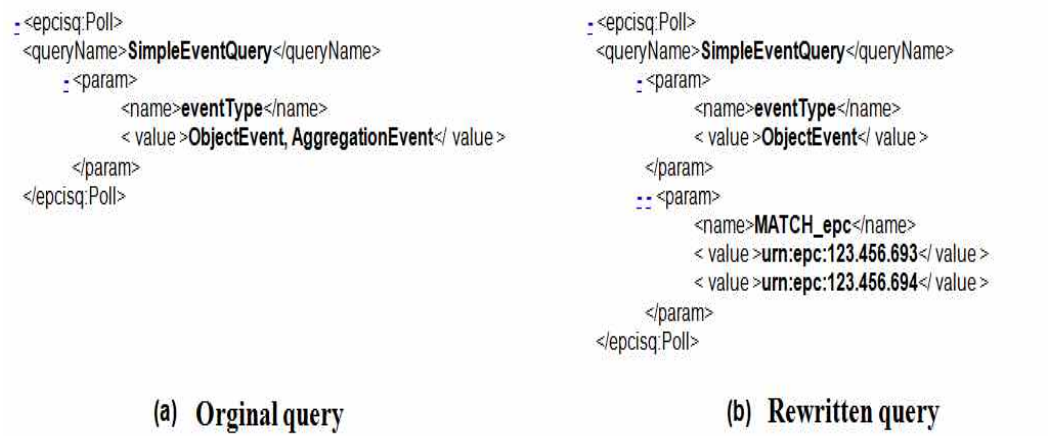
identical with received role in accessed EPCIS. It is difficult to determine role element in extended RBAC. To solve this problem, role mapping technology is applied in role translation across EPCISs. As shown in Figure 10, there are two role sets for EPCIS A and EPCIS B. The roles has hierarchy relationship on access right; Administrator > Salesman > Buyer > Gust. Dotted line denotes role mapping relationship between EPCIS A and EPCIS B. For example, administrator role in EPCIS A is same with manager role in EPCIS B. When user role administrator is transported from EPCIS A to EPCIS B, EPCIS B treats it as manager role. The accessible data code of manager is assigned to the user. Refer to [5] for more information on role mapping technology.

With user accessible tags and user role, user access right can be decided based on local policy of EPCIS. Figure 11 shows an example. When EPCIS B obtains registration information from EPCIS A, it can determine Bob's access right. Accessible tags are urn:epc:123.456.693 and urn:epc:123.456.694. Only RFID event data, which contains urn:epc:123.456.693 and urn:epc:123.456.694, are accessible for Bob. The Bob's role decides accessible event type and attributes based on EPCIS B local policy. Since



[Figure 11] User access right decision

Bob's role is buyer, its accessible data code is 100011000110 in EPCIS B. Bob only can access ObjectEvent which includes tag urn:epc:123.456.693 or tag urn:epc:123.456.693. Other type event data is not accessible. Furthermore, the attribute values of ObjectEvent are limited. Authorized ObjectEvent data only has recordTime, eventTime, readPoint and bizLocation attributes. Other attributes are limited for Bob.

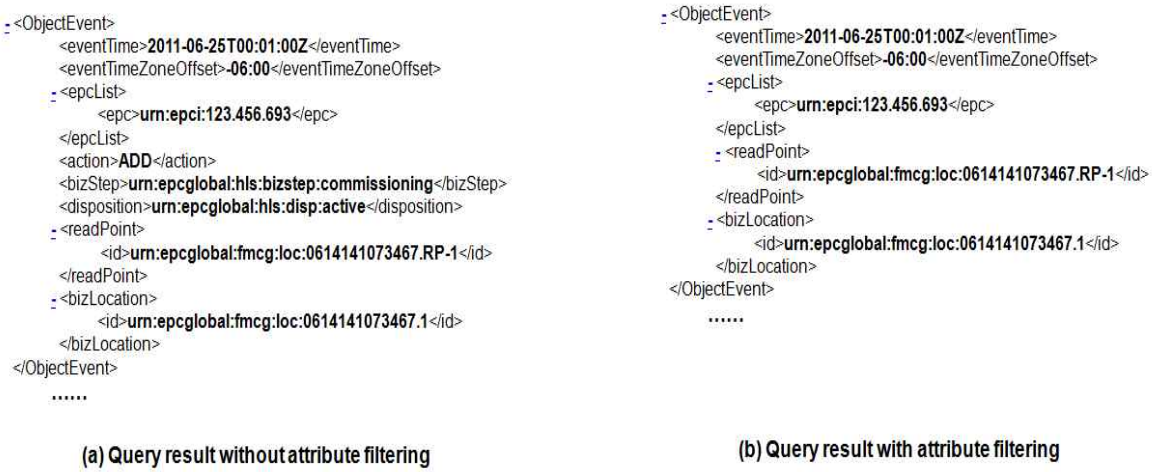


[Figure 12] Query rewritten example

5. Query processing for secure RFID data access

After user access right decision, user access right is represented as a set of tags and an accessible data code. Accessed EPCIS implements limited data access with access right by rewriting query parameters and filtering query result. Query parameters rewriting can address tag and event type access limitations. MATCH_epc query parameter is added in user query. It denotes equal predicate on epc attribute. If MATCH_epc is set as a tag's identification value urn:epc:123.456.693, the query result will only include RFID event data that includes tag urn:epc:123.456.693. Similarly, event type limitation can be addressed by setting eventType query parameter. EPCIS limits attributes access by result filtering. Result filtering deletes unauthorized attributes from query result.

For instance, Bob sends a query request to EPCIS B as figure 12 (a). This query has one query parameter eventType equal to ObjectEvent or AggregationEvent. Through access right decision, Bob can access ObjectEvent which include tag urn:epc:123.456.693 or tag urn:epc:123.456.694. AggregationEvent is not accessible for Bob. Before query processing, query is rewritten as (b) of figure 12. Eventtype equal to AggregationEvent is removed from eventType predicate. MATCH_epc is added to limit RFID tag access. The query result only



[Figure 13] Query filtering example

includes ObjectEvents and these event data has tag urn:epc:123.456.693 or tag urn:epc:123.456.694.

To limit unauthorized attributes access, query result is filtered to remove unauthorized attributes. Figure 13 shows a query result filtering example. Figure 13 (a) is query result of rewritten query. The result includes ObjectEvent which all attributes. Since only eventTime, recordTime, readPoint, bizLocation are accessible for Bob; bizStep and disposition attributes should be removed from query result. The figure 13 (b) is final result. Unauthorized attributes are not sent to user.

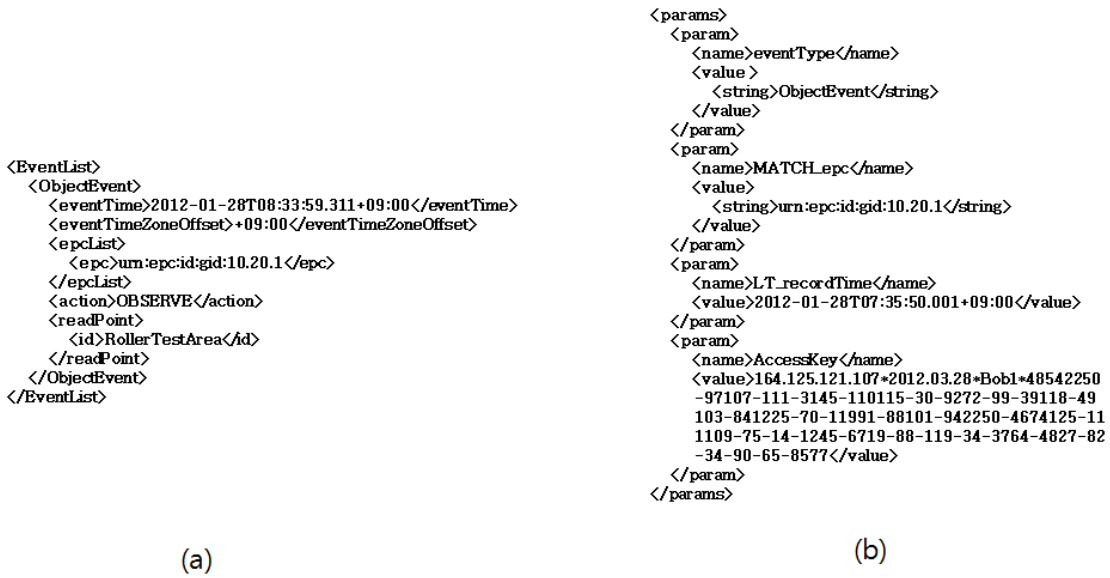
6. Experiments

In this section, some experiments are executed for evaluating EPCIS query processing performance and access control overhead. The experiments are executed on personal computers with 2.6GHz CPU, 2G main memory. The processing time is as performance metric for experiments.

6.1 Query and data set

Since there is no standard RFID business data set for EPCIS evaluation. We use the EPCIS event data generation tool to generate EPCIS data set [11]. The event data example is shown in Figure 14 (a). The benefit of generated EPCIS data set is easy to control data volume and data type. In following experiments, 50000 different types of RFID business events are stored in ten EPCISs.

In our experiments, we want to check overhead and query processing performance with different size of query result. Therefore, the defined queries should be with specific query result size. For simplify, EPCIS query includes EPC,



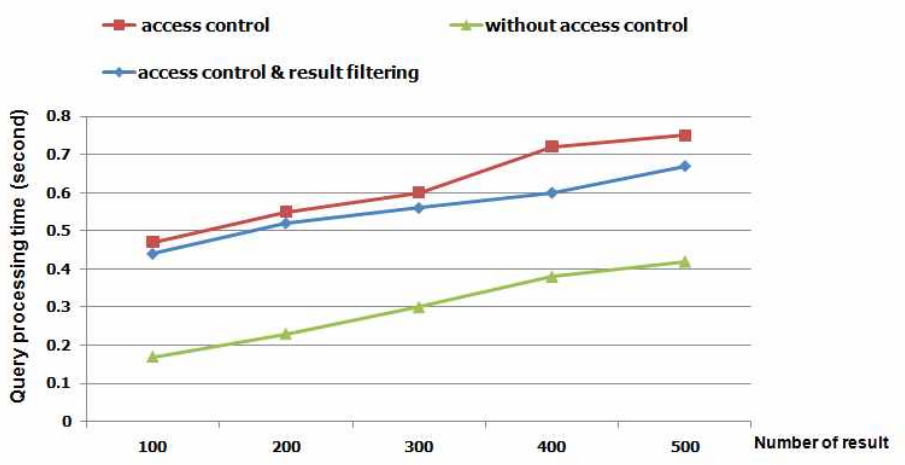
[Figure 14] Event data and query in experiments

eventType and recordTime three query parameters. Where recordTime is used to control query result size since recordTime attribute is EPCIS event timestamp in EPCIS.With such simple query parameter setting, we can easily check the correctness of query result. Since the access-key of user should be sent to EPCIS with query. Access-key is embedded in query as a parameter. Figure 14 (b) shows a query example which is used in our experiments.

6.2 Overhead evaluation

Three kinds of experiments are executed for checking overhead of proposed access control mechanism. First kind of experiment just executes query without access control processing. Second kind of experiment processes query with event level access control. Event level access control experiment process includes user authentication, authorization and query processing cost. While it does not include attribute filtering process. In order to evaluate overhead of access control query processing, first experiment and second experiment have same query result. Third kind of experiment process query with attribute level access control. Different with event level access control query processing, third kind of experiment's query result are filtered by access control limitation. Some attributes are removed from query result. The query result size is small than second set of experiments.

Figure 15shows evaluation result. Experiments without access control have best performance. Processing time of event level access control experiment is parallel to experiment without access control. Overhead is fixed regardless of number of query result. The overhead is



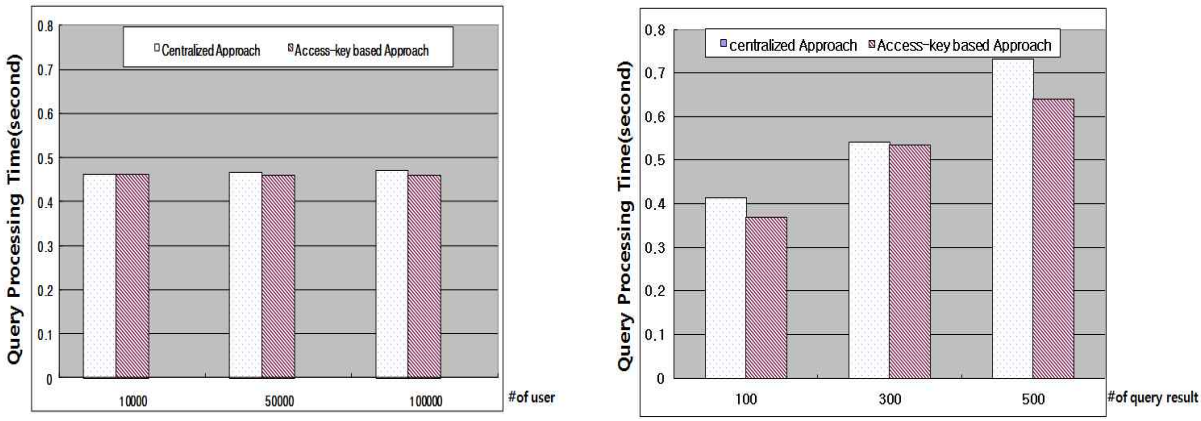
[Figure 15] Access control overhead evaluation result

generated by remote user authentication. Overhead of access control is about 0.3 in our experiment evaluation. Though having additional filtering cost, attribute level access control experiments have better performance than event level access control experiment. The reason is because the size of filtered query result is small; the network communication cost is reduced.

6.3 Query performance evaluation

After access control overhead evaluation, we do some experiments for comparing query processing performance under access-key based access control and centralized based access control. Same query set is executed over centralized access control implementation and our proposed access-key based access control implementation. Two kinds of experiments are done for query processing performance evaluation. First experiments are scale to number of users. With number of user increasing, the query processing performance has little different. In this case, user number is great different between access-key based implementation and centralized based implementation. In access-key based implementation, all user registered in ten distributed EPCISs, whereas, centralized implementation manages all users in centric server. The left one evaluation result of Figure 16reveals that the centralized access control implementation and access-key based access control implementation have similar performance even though the number of users are great different.

Second kinds of experiments are scale to number of query result. As shown in Figure 16. Access-key based access control has better performance than centralized access control implementation. Both of centralized access control and access-key based control need remote connection for authentication. They



[Figure 16] Query processing performance evaluation result

should have similar performance. However, in access-key based access control implementation, not all users require remote connection authentication. If registered EPCIS and accessed EPCIS are same one, the remote connection authentication is avoided. As summary, we know that the query performance mainly depend on number of query result. The number of user has little impact on query processing performance since database system can breezily process user information.

7. Conclusion

Basically, there are two approaches for distributed access control; centralized access controland cryptographic-key based access control. Centralized access control has a centric server for user authentication and authorization. There are two unsolved drawbacks in centralized model; first, it is performance bottleneck with too many user requests. Second, when the centric server is broken, it takes the whole authentication and authorization system with it. And, cryptographic-key based access control has complex key management problem. In this study, we propose access-key based access control mechanism. It efficiently realizes access control for distributed EPCISs data accessing. Both authentication and authorization are addressed based onaccess-key in this mechanism. Access-key is used to index user registration information which is used to decide user access right. Signature of access-key can address user authentication. Moreover, accessible data code is designed to present user role permission. At last, a set of experiments are executed to verify the efficiency of proposed access control mechanism. Compare with centralized access control, it enhances access control availability. Since every EPCIS is to authenticate its own users, even some EPCISs are broken, other EPCISs are not affected. There is no complex cryptographic-key

management problem since each EPCIS only need to verify its own signature. However, access-key based mechanism brings key management problem for users. One user may be registered in several EPCISs; the user has to keep a lot of access-keys for all registered EPCISs. It is inconvenient to users.

For future work, we need to consider the access-key management. Additionally, only EPCIS access control is studied in this paper. Other EPCglobal network components security also needs to be considered for providing completely secure RFID system.

8. Reference

[1] K. Domdouzis, B. Kumar, C. Anumba. "Radio-Frequency Identification (RFID) Applications: A Brief Introduction," *Advance Engineering Informatics*, vol.21, pp. 350-355, 2007.

[2] F. Niederman, R.G. Mathieu, R. Morley, I. Kwon. "Examining RFID Applications in Supply Chain Management," *Communications of ACM*, vol. 50, pp. 92-101, 2007.

[3] EPCglobal. "EPC Information Services Version 1.0.1 Specification. EPCglobal Standard Specification," http://www.gs1.org/gsmp/kc/epcglobal/epcis, 2007.

[4] E. Grummt, M. Muller. "Fine-Grained Access Control for EPC Information Services," *IOT'08 Proceedings of the 1st international conference on the internet of things*, pp. 35-49, 2008.

[5] A. Kapadia, J. Al-Muhtadi, R.H. Campbell, D. Mickunas. "IRBAC 2000: Secure Interoperability Using Dynamic Role Translation," *Technical Report:UIUCDCS-R-2000-2162*, 2000.

[6] B. Shafiq, B.D. Joshi. "Secure Interoperation in a MultidomainEnvironment Employing RBAC Policies," *IEEE Transactions on Knowledge and Data Engineering*, vol. 17, pp. 1557-1577, 2005.

[7] Wenyan Yu, Yongxu Piao, Joonho Kwon, Bonghee Hong. "Access key based Distributed Secure Access Control for EPCglobal Networking," *The Third International Conference on Emerging Database*, pp. 188-199, 2011.

[8] D.F. Ferraiolo, R. Kuhn, R. Chandramouli. "Role-Based Access Controls," *Artech House*, 2003.

[9] R.D. Sandhu, E.J. Coyne, H.L. Feinstein, C. E. Youman. "Role-Based Access Control Models," *IEEE Computer Society Press*, vol. 29, pp. 38-47, 1996.

[10] EPCglobal. "EPCglobal Architecture Framework,"http://www.gs1.org/gsmp/kc/epcglobal/architecture, 2010.

[11] Taihyun Ahn, Joonho Kwon, Bonghee Hong. "Implementation of Generating Data Tool for EPCIS and EPCDS," *Information Systems International Conference*, pp. 51-55, 2011.

박 영 욱

2003년 중국 연변대학교 컴퓨터공학과 졸업(학사)

2006년 중국동북사본대학교 컴퓨터공학과 졸업(석사)

2006년 – 현재 부산대학교 컴퓨터공학과 박사과정

관심분야 : RFID 미들웨어, 스트림 데이터처리, RFID 보안 등

류 우 석

1997년 부산대학교 컴퓨터공학과 졸업(학사)

1999년 부산대학교 컴퓨터공학과 졸업(석사)

2012년 부산대학교 컴퓨터공학과 졸업(박사)

2012년 – 현재 부산대학교 컴퓨터공학과 박사후연구원

관심분야 : RFID 미들웨어, ALE, 태그 데이터 모델, RFID 트랜잭션, 미들웨어 테스팅 모델 등

우 문 언

2009년 중국 동북대학교 컴퓨터공학과 졸업(학사)

2011년 부산대학교 물류IT학과 졸업(석사)

2011년 – 현재 중국 InterActiv Corp. Program Manager

관심분야 : RFID 미들웨어, RFID 보안 등

권 준 호

1995년 서울대학교 컴퓨터공학과 졸업(학사)

1999년 서울대학교 전기, 컴퓨터공학과 졸업(석사)

2009년 서울대학교 전지, 컴퓨터공학과 졸업(박사)

2010년 – 현재 부산대학교 물류IT협동과정 교수

관심분야 : RFID 미들웨어, 데이터베이스, 물류정보 시스템 등

홍 봉 희

1982년 서울대학교 컴퓨터공학과 졸업(학사)

1984년 서울대학교 컴퓨터공학과 졸업(석사)

1988년 서울대학교 컴퓨터공학과 졸업(박사)

1987년 – 현재 부산대학교 정보컴퓨터공학부 교수

관심분야 : RFID 미들웨어, 데이터베이스, 실시간 위치 정보 시스템, 유비쿼터스 미들웨어 등