

Singapore Management University Institutional Knowledge at Singapore Management University

Research Collection School Of Information Systems

School of Information Systems

4-2012

Evaluation of Different Electronic Product Code Discovery Service Models

Su Mon KYWE

Singapore Management University, monkywe.su.2011@phdis.smu.edu.sg

Jie SHI

Singapore Management University, jieshi@smu.edu.sg

Yingjiu LI


Singapore Management University, yjli@smu.edu.sg

Raghuwanshi KAILASH

Singapore Management University, kailashr@smu.edu.sg

DOI: <https://doi.org/10.4236/ait.2012.22005>

Follow this and additional works at: https://ink.library.smu.edu.sg/sis_research

 Part of the [Information Security Commons](#), and the [Operations and Supply Chain Management Commons](#)

Citation

KYWE, Su Mon; SHI, Jie; LI, Yingjiu; and KAILASH, Raghuwanshi. Evaluation of Different Electronic Product Code Discovery Service Models. (2012). *Advances in Internet of Things*. 2, (2), 37-46. Research Collection School Of Information Systems.

Available at: https://ink.library.smu.edu.sg/sis_research/1631

This Journal Article is brought to you for free and open access by the School of Information Systems at Institutional Knowledge at Singapore Management University. It has been accepted for inclusion in Research Collection School Of Information Systems by an authorized administrator of Institutional Knowledge at Singapore Management University. For more information, please email libIR@smu.edu.sg.

Evaluation of Different Electronic Product Code Discovery Service Models

Su Mon Kywe, Jie Shi, Yingjiu Li, Raghuwanshi Kailash

School of Information Systems, Singapore Management University, Singapore City, Singapore

Email: {monkywe.su.2011, jieshi, yjli, kailashr}@smu.edu.sg

Received December 21, 2011; revised January 19, 2012; accepted February 4, 2012

ABSTRACT

Electronic Product Code Discovery Service (EPCDS) is an important concept in supply chain processes and in Internet of Things (IOT). It allows supply chain participants to search for their partners, communicate with them and share product information using standardized interfaces securely. Many researchers have been proposing different EPCDS models, considering different requirements. In this paper, we describe existing architecture designs of EPCDS systems, namely Directory Service Model, Query Relay Model and Aggregating Discovery Service Model (ADS). We also briefly mention Secure Discovery Service (SecDS) Model, which is an improved version of Directory Service Model with a secure attribute-based access control mechanism. Then, we analyze the strengths and limitations of these models, by comparing based on non-functional features such as data ownership, confidentiality, business relationship independence, availability, reliability, implementation complexity, visibility, and scalability. From the analysis results, we have a better understanding of which model is more suitable in what kinds of situations or scenarios. Moreover, we suggest possible improvements and identify possible future add-on applications to SecDS model in the paper.

Keywords: EPC Discovery Service; Supply Chain; Access Control; Comparison

1. Introduction

Supply chain is a process of transforming natural resources or raw materials into finished goods, by passing through suppliers, manufacturers, wholesalers, retailers, customers and other supply chain partners [1]. When various supply chain partners work together to deliver the right amount of goods to the right customers at right time and right place, good coordination and information sharing are critical.

Lack of information sharing among supply chain partners can lead to a lot of negative consequences. For instance, when downstream retailers are not willing to share their end customer information (e.g. for security and privacy reasons), upstream suppliers and manufacturers have no idea about the customers. The manufacturers predict the customer demand from wholesalers' orders, while wholesalers predict the customer demand from the retailers' orders. This lack of information transparency can lead to "bullwhip effect" where each upstream supply chain participant observes greater demand variation and greater need for safety stocks, consequently bearing greater costs [2]. The whole supply chain can suffer as it becomes less responsive to demand fluctuations.

Therefore, in today's market where competition is

very intense, it becomes increasingly important to have a structured way of fast and secure information sharing among supply chain partners. Standardized systems and communication methods, which can be used uniformly across different organizations around the globe, are required to be developed.

As such, EPCglobal organization [3], which is responsible for standardization of Electronic Product Code (EPC) technology [4], created EPCglobal Network [5] for sharing RFID information. EPCglobal Network is implemented, using standards from EPCglobal Architecture Framework [6]. It has four components, namely Object Naming Service (ONS), EPC Discovery Services (EPCDS), EPC Information Services (EPCIS) and EPC Security Services [5]. In this paper, we focus mainly on EPCDS models, since standardization of EPCDS design is still an open research question [6].

Our paper is structured as follows. Section 2 provides background information on EPCDS and EPCIS. Section 3 briefly describes existing EPCDS models which include Directory Service Model, Query Relay model and Aggregating Discover Service model. In Section 4, we describe SecDS model which is an extension of Directory Service Model. Section 5 gives comparison of the different models and Section 6 summarizes the analysis. Then, we identify possible improvements for SecDS model in

Section 6 and finally we conclude the paper in Section 7 with the role of EPCDS in future Internet of Things (IOT) [7].

2. Background

2.1. EPCDS

Electronic Product Code Discovery Service (EPCDS) is a service that allows users to find supply chain partners who possess a given product. A user just need to key in a particular EPC number, such as RFID number of the product, to search for EPC Information Services (EPCIS) provided by the related supply chain partners within the network.

EPCDS can be compared to telephone directory or search engines of the internet. To request information about a particular EPC, a supply chain participant needs to have knowledge of who are its supply chain partners and their network addresses or URLs that should be queried. This is like the need to know the phone numbers before contacting each other. Then, EPCDS acts like a telephone directory or yellow page where the contacts or addresses of EPC information providers or repositories are aggregately stored and returned to the appropriate queries accordingly, as shown in **Figure 1** [8].

Basically, EPCDS supports two operations, publishing operation and querying operation. Publishing operation is for EPCIS to publish their information on EPCIS whereas querying operation is for supply chain users, who want to find published EPCIS addresses.

2.2. EPCIS

In this context, EPC Information Service (EPCIS) can simply be viewed as a database or repository owned by a supply chain participant. It stores event information of supply chain products, where each product is uniquely identified by an EPC number. EPC event information includes product information, product location, date and time of product arrival and departure, involved business processes, and other important business information [6].

To share its critical business information with its trusted supply chain partners, EPCIS provides a querying

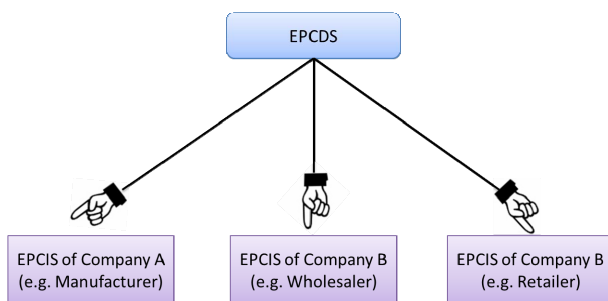


Figure 1. EPCDS as a directory of EPCIS.

interface for its repository. However, EPCIS may maintain access control mechanisms to ensure that only authorized users can access its sensitive information. With EPCIS querying service, any authorized users, who know the address of EPCIS service, can get access to its EPC repositories or databases easily.

2.3. Definition of Terms

In our paper, the terms “users” or “clients” is used for supply chain participants who want to get EPC event information from EPCIS. EPCIS company (owner), database and its services are collectively mentioned as “EPCIS”, “resource”, “EPCIS resource” “EPCIS repository” or “EPCIS company”.

3. Existing Discovery Service Models

BRIDGE (Building Radio frequency identification for the Global Environment) project has modeled and analyzed eight possible high level designs of EPCDS in 2007. After considering each model’s feasibility, BRIDGE selected the two models of EPCDS, called Directory Service Model and Query Relay Model [8]. Although there are a lot of variations of these two models, our paper only use basic models suggested in BRIDGE document for simplicity purpose. The third EPCDS design is Aggregating Discovery Service (ADS) Model, proposed by Hasso Plattner Institute for IT Systems Engineering in 2010 [9].

3.1. Directory Service Model

In Directory Service Model, EPCDS stores a directory of EPC numbers and corresponding EPCIS addresses. **Figure 2** illustrates the steps of this Directory Service Model.

Step 1: An owner of an EPCIS first registers at EPCDS with the details on which EPC numbers they are handling, together with its service address or URL. EPCDS stores the pairs of EPC numbers and EPCIS addresses in its lookup table.

Step 2: User sends query to EPCDS with a specific EPC number or a range of EPC numbers as parameters.

Step 3: EPCDS uses lookup table to look up queried EPC numbers, finds corresponding EPCIS addresses and returns them to the user.

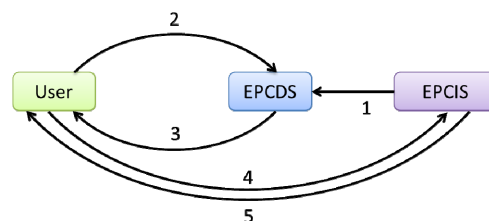


Figure 2. Steps in Directory Service Model.

Step 4: With the returned addresses, the user queries directly to EPCIS repositories to get the desired required EPC event information.

Step 5: EPCIS repositories return the required EPC event information to the user.

One of the main problems of Directory Service Model is that EPCDS returns all the related EPCIS addresses to every user who queries. Access control mechanisms are not specified in detail.

Based on the query result, every user knows exactly which EPCIS repositories are handling which EPC numbers. Availability of EPCIS addresses indicates ownership of product information in that EPCIS companies. Therefore, many companies, who consider their possession of items as confidential or sensitive information, do not want to expose their EPCIS addresses and are reluctant to publish them on EPCDS.

3.2. Query Relay Model

In the query relay model, EPCDS does not return the service addresses of EPCIS repositories immediately upon request. Instead, it redirects the query to corresponding EPCIS repositories which have their own access control mechanisms. As shown in **Figure 3**, query relay model has the following steps.

Step 1: An owner of an EPCIS first registers at EPCDS with the details on which EPC numbers they are handling, together with its service address or URL. Then, EPCDS stores the pairs of EPC numbers and EPCIS addresses in the lookup table.

Step 2: User sends query to EPCDS with a specific EPC number or a range of EPC numbers as well as user's credentials as parameters.

Step 3: EPCDS uses lookup table to look up queried EPC numbers, finds corresponding EPCIS addresses and relays user's query and credentials to those EPCIS resources.

Step 4: Each EPCIS resource checks user's credentials against its own access control database and returns the query result to the authenticated user directly.

Actually, in query relay model, user query can be of two types. The first one is a full query, directly requesting EPCIS to return the full EPC event information. The second query type is a resource query, where EPCIS returns only the service address that user should query to

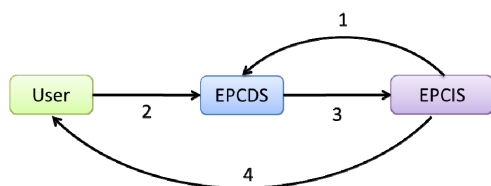


Figure 3. Steps in query relay model.

get required EPC event information.

3.3. Aggregating Discovery Service (ADS)

Aggregating Discovery Service (ADS) model is based on the query relay model. In this model, instead of returning EPC event information directly to user, each EPCIS returns the result back to EPCDS. Only after getting replies from different EPCIS repositories, EPCDS aggregates their information and sends them back to the user. **Figure 4** shows the steps of aggregating discovery service model.

Step 1: An owner of an EPCIS first registers at EPCDS with the details on which EPC numbers they are handling, together with its service address or URL. Then, EPCDS stores the pairs of EPC numbers and EPCIS addresses in the lookup table.

Step 2: User sends query to EPCDS with a specific EPC number or a range of EPC numbers as well as user's credentials as parameters.

Step 3: EPCDS uses lookup table to look up queried EPC numbers, finds corresponding EPCIS addresses and relays user's query and credentials to those EPCIS resources.

Step 4: Each EPCIS resource checks user's credentials against its own access control database and returns the query result to EPCDS.

Step 5: EPCDS aggregates the results and relays them back to the user.

4. Secure Discovery Service Model

Secure Discovery Service model (SecDS) is based on Directory Service Model.

As described in Section 3.1, Directory Service Model has a critical problem due to the lack of access control system in EPCDS. Sensitive business information may be leaked, since EPCDS returns related EPCIS addresses to every user query.

In SecDS model, the basic Directory Service Model is improved by implementing a secure access control mechanism inside EPCDS. Access control mechanism in EPCDS makes sure that it does not release EPCIS addresses to any unauthorized users. Confidentiality of important EPC information is preserved.

As shown in **Figure 5**, steps in SecDS model are the same as steps in Directory Service Model, except that in

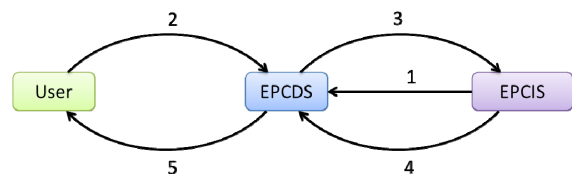


Figure 4. Steps in aggregating discovery service model.

step 1, access control policies are sent together with EPC numbers and EPCIS address from EPCIS. In addition to lookup table of EPCIS addresses, EPCDS maintain a database on access control policies in SecDS model.

Moreover, EPCDS provides interfaces for adding, deleting and modifying access control policies. EPCIS owners can use these interfaces to synchronize access control polices between EPCDS and EPCIS.

4.1. Architecture of SecDS Model

Figure 6 describes the overview EPCDS architecture of SecDS model with attribute-based access control system [10].

4.1.1. Data Storage

Data storage component contains event information related to EPC numbers. The attributes of the table are EPC number, EPCIS address, Published Date and Time, as well as other Publisher information. These attributes can be used to define access control polices in EPCDS.

4.1.2. Policy Storage

Policy storage component contains two types of access control policies for EPCDS. One is for publishing and another is for querying.

Policies for publishing determine who can publish access control policies in EPCDS and are managed by security administrators of EPCDS. On the other hand, policies for querying are defined by security administrators

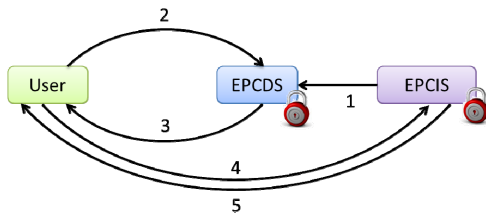


Figure 5. Steps in secure discovery service model.

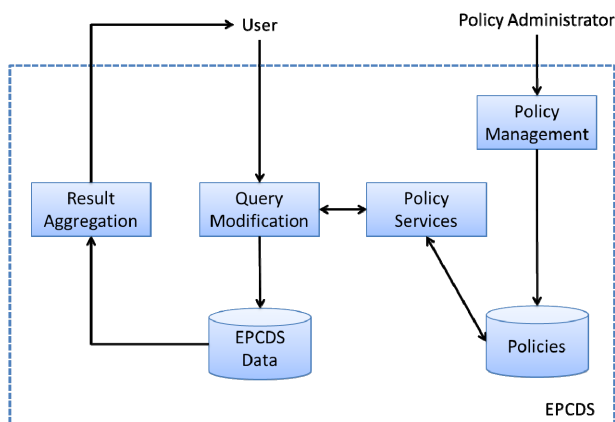


Figure 6. Architecture of EPCDS in SecDS model.

of each EPCIS and are used to control who is able to query its EPC event information. Complexity of SecDS model lies in managing policies for querying because attribute-based access control is needed for querying users. The policies for publishing are simple Role-Based Access Control (RBAC).

4.1.3. Policy Management

Policy management component provides an interface for EPCIS owner to publish, update or delete their policies on EPCDS. It performs syntax analysis, semantic analysis and policy transformation before saving the policies in policy storage database.

Syntax and semantic analysis checks the syntax and semantic of submitted policies while policy transformation transforms attribute-based access control policies into fine-grained access control policies. The purpose of transformation is to improve the efficiency of querying. However, the trade-off is the increased complexity of maintaining the policies.

4.1.4. Policy Services

Policy service component supports query modification component. Whenever there is a query, policy service component searches for related fine-grained access control predicates, combines them into one access control policy and returns it to query modification component.

4.1.5. Query Modification

Query modification component changes normal queries into modified queries that comply with the access control policies.

4.1.6. Result Aggregation

Result aggregation component returns the aggregated EPCIS addresses to the user. With the returned EPCIS addresses, user can then query to EPCIS companies directly to get EPC information. User may also store the EPCIS addresses and in the future, query to EPCIS repositories without the need to interact with EPCDS again.

4.2. Attribute-Based Access Control of SecDS Model

The main contribution of SecDS model lies in its secure attribute-based access control system, where each EPCIS owner can set his own access control policies based on certain attributes. Attribute-based access control (ABAC) is chosen, despite its complexity, because it is more flexible than other access control systems and fulfills the business needs and requirements of supply chain information sharing.

For instance, an EPCIS owner can define that certain EPC numbers are accessible, depending on the role at-

tribute of the users (e.g. a manufacturer, wholesaler or retailer) and/or the time attribute of EPC events (e.g. after 5/11/2011). Generally, there are three types of attributes with which an EPCIS can define access control policies.

Subject Attribute: Subject attributes are properties related to user companies such as Company ID, Company Name, Company Role, Company Location (Country, City, etc).

Object Attribute: Object attributes are properties of EPC events such as EPC Number, Time, and Business Process.

Visibility Attribute: Three types of visibility attributes can be used, namely whole-stream, up-stream and down-stream attribute.

In whole-stream policy, information related to an EPC number can be accessed by users of any companies who also publish event information about the same EPC number. Intuitively, it means that companies which handle the same product along the whole supply chain are allowed to access information about that product.

In up-stream policy, the information related to an EPC number can be accessed by users of any companies who handle the same EPC number before the publishing EPCIS does. For example, in a supply chain of supplier, manufacturer, distributor, wholesaler and retailer, the distributor's EPC information can be accessed by the supplier and the manufacturer of the same product.

In down-stream policy, the information related to an EPC number can be accessed by users of any companies who handle the same EPC number after the publishing EPCIS does. In the above supply chain, the distributor's information can be accessed by the wholesaler and the retailer of the same product.

These attribute-based access control policies are maintained in EPCIS companies and synchronized with EPCDS all the time.

5. Comparison of Different EPCDS Models

There have been research papers on the comparisons of different EPCDS models using different requirements. In [11], basic requirements for EPCDS design are identified to compare Directory Service Model and Query Relay model. The requirement features include data ownership, security (confidentiality, reliability and availability), business relationship independent design, organic growth, scalability and quality of service.

[9] uses the same requirements from [11] but they suggested Aggregating Discovery Service model and included it in the comparison. [12] compares scalability of Directory Service model and Query Relay model using supply chain simulation. [13] provides a consolidated comparison of Discovery Service architecture designs of

EPCglobal [6], BRIDGE project [8], Afiliis [14], ID@URI naming system [15] and Distributed Hash Table DHT-based Discovery Service [16], based on the requirements from the ISO/IEC 9126 [17] standard, BRIDGE project [8] as well as [11].

Our paper reuses the basic requirements described in [11] and adds in more features to evaluate Query Relay model, Aggregating Discovery Service model and SecDS model. Since SecDS model is an improvement of Directory Service model, we do not include the latter in our comparison.

The requirements are rated as "high", "medium" or "low", indicating that the model highly fulfills, moderately fulfills or almost does not fulfill the requirements.

5.1. Data Ownership

Data ownership is defined as the right to determine data usage privileges to other companies and as the ability to track the actual usage. EPCIS companies should have complete control over its data such as EPCIS address, EPC event information, business data as well as the settings of access control rights.

In [10], it is assumed that data ownership is lost once EPCIS delegates access controls to EPCDS. However, in our analysis, we assume that EPCDS is trusted and always acts in the way that it is supposed to. It does not expose the EPCIS addresses, returned results or published policies to any unauthorized persons.

5.1.1. Right to Determine Data Usage Privileges

Query Relay Model: This requirement is highly fulfilled since EPCIS manages its own access control policies and has local control over its EPC event information. It can also determine who can access to its EPCIS address.

Aggregating Discovery Service Model: Like query relay model, this requirement is also fulfilled in ADS model because EPCIS manages its own access control policies and possesses the ability to determine who has access to its EPC event information.

Secure Discovery Service Model: In SecDS model, EPCIS needs to publish some of its data attributes on EPCDS to support attribute-based access control policies. However, EPCIS can set the access control policies in EPCDS for their data. This requirement is fulfilled, assuming that access control policies in EPCDS works perfectly and that EPCDS is completely secured and trusted, in a sense that no unauthorized persons has access to the EPC event information.

5.1.2. Ability to Track Data Usage

Query Relay Model: This requirement is completely fulfilled as EPCDS can track who queries its service ad-

dress and data.

Aggregating Discovery Service Model: This requirement is completely fulfilled since every query is handled by EPCDS in ADS model.

Secure Discovery Service Model: This requirement is only partially fulfilled in SecDS model. The reason is that EPCIS can track who is querying what EPC event information but EPCIS does not know who is given its EPCIS address until the user issues a query to the resource.

Although EPCIS has published policies on who can access its EPCIS address, this only ensures the confidentiality of EPCIS address. It does not support any tractability of who is given EPCIS address.

5.2. Confidentiality

Confidentiality is defined as preventing information from unauthorized access. In the following analysis, we assume that communication channel is secure and no adversary can eavesdrop or perform traffic analysis on the network channels. The only potential adversaries are users or EPCIS resources.

5.2.1. Client Confidentiality

Client confidentiality refers to unrevealing of any user query to irrelevant resources. Client confidentiality is important because user query reflects the strategic intentions or aims of the user. Client's query for EPC event information should be treated as sensitive information.

Query Relay Model: In query relay model, EPCSD relays client queries directly to EPCIS resources. The user does not have a chance to check the EPCIS addresses. Therefore, the user's interested EPC numbers as well as query details may be released to unrelated EPCIS resources. Client confidentiality is low in this model.

Aggregating Discovery Service Model: Like query relay model, EPCDS relays user query directly to the registered EPCIS resources. Therefore, client confidentiality is also low in ADS model.

Secure Discovery Service Model: In SecDS model, the user can get the EPCIS addresses first and check if the addresses are in user's blacklist which contains addresses of competitors and dubious resources. Only if they are not in the blacklist, user can direct its queries to them. Client confidentiality of SecDS model can be rated as medium as there are still chances that client queries are leaked to irrelevant resources which are not in the blacklist.

5.2.2. Resource Confidentiality

Resource confidentiality refers to unrevealing of EPC event information and EPCIS addresses to unauthorized users. Resource confidentiality is assured in all three

models since they all do not release EPCIS address and EPC event data to unauthorized users.

5.3. Availability and Reliability

Availability is defined as a system's immediate readiness for usage whereas reliability refers to continuity of service over a prolonged period of time.

Query Relay Model: When resources query is used in query relay model, EPCIS address is returned to the user. Whenever user needs to query EPCIS, user can just reuse the address from cache. User does not need any help from EPCDS to get the desired result. So, even when EPCDS is down, user's request can be fulfilled by EPCIS. Therefore, availability and reliability is high in query relay model.

Aggregating Discovery Service Model: In this model, EPCDS is a single point of failure. Once EPCDS is unavailable, users have no way of communication with EPCIS resources as users do not have any information about EPCIS addresses. So, we can conclude that availability and reliability of this model is lower than that of query relay model and SecDS model.

Secure Discovery Service Model: Since SecDS model returns EPCIS addresses to user, like query relay model, the same argument from query relay model goes for high availability and reliability in SecDS model.

5.4. Complexity

Complexity refers to difficulty of implementing and maintaining a system. It indicates time and effort that should be put in to use the services provided by the system.

5.4.1. Client Complexity

Client complexity is the implementation effort that client needs to put in to be able to get the required EPC event information.

Query Relay Model: Normally, firewall matches the returning addresses with outbound addresses. However, in query relay model, request is sent to EPCDS while a number of EPCIS replies to the user. So, client needs a proxy which allows incoming traffic from unknown addresses. Client also needs to inspect the response by checking the session identifier.

Moreover, since client has no information on the number of relevant EPCIS resources, it does not know how many responses will be. Therefore, client query needs to maintain an open connection state and waits for a certain period of time before time out. This asynchronous connection makes client complexity high in query relay model.

Aggregating Discovery Service Model: In ADS model, client complexity is low since EPCDS returns the aggregated EPC event information directly.

Secure Discovery Service Model: In SecDS model, complexity is medium as EPCDS only provides services to find the EPCIS addresses. Client itself needs to implement a system to query to EPCIS resources and aggregate the results to get the required information.

5.4.2. EPCDS Complexity

EPCDS complexity refers to the development and maintenance effort of EPCDS.

Query Relay Model: Implementation in EPCDS is less complex in query relay model. This is because EPCDS only needs to maintain a lookup table and relay any query accordingly.

Aggregating Discovery Service Model: Complexity level of EPCDS in ADS model is high. It needs to maintain a number of connections or states of queries while connecting to a number of EPCIS. Furthermore, EPCDS needs to aggregate the results before sending back to the user. The cost for query processing and maintaining a number of connections is high.

Secure Discovery Service Model: In SecDS model, complexity of maintaining fine-grained access control policy is very high. With every update, delete or publish activity, a lot of processing is needed to transform from attribute-based access control to fine-grained access control.

5.4.3. Resource Complexity

Resource complexity is the effort that EPCIS resource needs to maintain.

Query Relay Model: EPCIS resource only needs to maintain its own access control policies and returns EPC event information to authorized users. Therefore, resource complexity is medium in query relay model.

Aggregating Discovery Service Model: It is the same as query relay model.

Secure Discovery Service Model: Resource complexity is relatively high, compared to query relay model and ADS model. The reason is that in addition to maintaining its own access control database, each EPCIS resources needs to make sure that its access control policies are duplicated at the EPCDS level. Whenever there are changes in business relationship, access control policies need to be updated and synchronized in EPCDS.

5.5. Scalability

Scalability refers to the ability to handle large amount of user queries and data. EPCDS should be able to support increasing network traffic in terms of both user volume and data volume. The scalability of EPCDS is highly correlated with the complexity of managing EPCDS.

Query Relay Model: Scalability is not much of an issue in query relay model. Data volume and query proc-

essing can increase gradually with the increased number of users.

Aggregating Discovery Service Model: Scalability is one of the main problems of ADS model. As the number of user queries increases, EPCDS needs to handle a lot more increased connections to EPCIS resources and processing of the results.

Secure Discovery Service Model: Scalability is also an issue in SecDS model. With the increased EPCIS resources registering at EPCDS, a lot more fine-grained access control policies need to be stored. These policies should be retrieved and processed for each query. Moreover, as the queries need to be modified according to the access control policies, processing load will increase significantly with increased number of queries.

5.6. Independence of Business Relationship

In supply chain where business relationships and partnerships are unstable, it is important to have EPCDS mechanisms which are independent of those business relationships.

Query Relay Model: In query relay model, EPCDS is independent on the business relationships of supply chain participants. Change in business relationships affects only the local access control policies of EPCIS resources.

Aggregating Discovery Service Model: The same argument goes for ADS model.

Secure Discovery Service Model: SecDS model is dependent on business relationships. Every time there is a change in partnerships, access control policies in EPCDS should also be updated immediately.

5.7. Quality of Service

Quality of service can be measured as the completeness and correctness of the result returned to the user.

Query Relay Model: In query relay model, EPCDS does not give user any information about the total number of EPCIS resources that is relevant to the user query. Consequently, if an EPCIS does not reply due to error or unavailable service for a short period, user may just assume that that EPCIS does not exist. Therefore, completeness of query result is not assured in this model.

Aggregating Discovery Service Model: In ADS model, EPCDS replies the aggregated query result to the user, including the EPCIS resources which are relevant to user query but cannot return information to the query due to error or unavailable service. Even though user cannot get the complete result this time, user can still query again later to get complete information.

Secure Discovery Service Model: Like ADS model, SecDS model also supports completeness and correctness of the query result. Since EPCDS in SecDS model returns all the relevant EPCIS addresses, user know exactly

which EPCIS does not response and query again later.

5.8. Visibility

Visibility refers to the amount of observation and assessment that an EPCDS can make on the performance of the overall system. It is important for EPCDS to make sure registered EPCIS resources are really fulfilling user's information need. High visibility on the whole system can leads to improved service fulfillment as well as quality assurance.

Query Relay Model: The visibility of EPCDS is low in query relay model because EPCDS just relays the query to EPCIS and EPCIS itself replies the results to the user directly. EPCDS has no clue on whether an EPCIS address is still working and replying to user queries or whether the service is really fulfilled.

Aggregating Discovery Service Model: In ADS model, EPCDS has high visibility as EPCDS is responsible for aggregating query results for the users. EPCDS can even track the up and down times of EPCIS resources as well as their performance and efficiency in replying user queries.

Secure Discovery Service Model: Like query relay model, SecDS model also returns the EPCIS addresses only. SecDS model does not know whether an EPCIS address is still valid and working. EPCDS cannot track if the users actually get the information that is needed. Therefore, the visibility is low in SecDS model.

6. Discussion

Table 1 below provides a summarized comparison between query relay model, aggregating discovery service (ADS) model and SecDS model.

Query relay model performs well in all areas, except

its high client complexity, low client confidentiality, low EPCDS visibility and low quality of service. This model is generally good for both EPCDS and EPCIS companies because it provides less implementation complexity and high scalability for EPCDS as well as great data ownership and confidentiality for EPCIS. The only potential problem is that EPCDS may not be able to track its service fulfillment. Nonetheless, the user may be reluctant to use the service of this model since it requires user's complex system implementation but does not guarantee user's confidentiality and completeness of query result.

On contrary to query relay model, Aggregating Discovery Service (ADS) model has high quality service for user and high visibility for EPCDS. It also provides high data ownership and confidentiality of EPCIS companies. Nevertheless, client confidentiality is not assured and EPCDS is a single-point-of-failure in this model. EPCDS also needs to bear high maintenance cost and scalability is an issue for EPCDS.

SecDS model is generally good in terms of data ownership and confidentiality for all EPCIS companies and users. Like query relay model, it provides reliable service with good quality and high visibility. However, it has high complex implementation for users, EPCIS as well as EPCDS. As a result, scalability is a big issue in SecDS model.

7. Possible Future Improvements to SecDS Model

7.1. Policy Synchronization

In SecDS model, access control policies should be duplicated and synchronized perfectly between EPCIS and EPCDS.

However, in the current implementation, only the pol-

Table 1. Summary of requirement analysis.

Assessed Features	Query Relay Model	ADS Model	SecDS Model
Data Ownership: Right to Determine Data Usage Privileges	High	High	High
Data Ownership: Ability to Track the Usage	High	High	Medium
Client Confidentiality	Low	Low	Medium
Resource Confidentiality	High	High	High
Availability and Reliability	High	Low	High
Client Complexity*	High	Low	Medium
EPCDS Complexity*	Low	High	High
Resource Complexity*	Medium	Medium	High
Scalability	High	Low	Low
Independent of Business Relationship	High	High	Low
Quality of Service	Low	High	High
Visibility	Low	High	High

*Although "High" indicates positive assessment in features like data ownership and confidentiality, "High" level of implementation complexity stands for negative evaluation of the feature.

icy administrator in EPCIS can publish policies to EPCDS while normal publisher cannot. This indicates that there may be some delay in publishing EPC event data and policies. In this delayed time window, any users can query the EPC event information. The formal implementation of SecDS model will enable that every normal publisher of EPC information can also publish related policies immediately.

Moreover, as policy publishing and data publishing are two separate operations in SecDS model, there is still a risk of resource forgetting to publish access control policies after publishing data. This can also lead to exposing sensitive information to random users. SecDS model should make it mandatory for every user who publishes event data to simultaneously publish related access control policies.

7.2. Improved Tractability and Data Ownership

As mentioned in Section 5.1.2., the current implementation of SecDS model does not provide any traceability functions for EPCIS resources to track who has queried its EPCIS address. It would be nice to have such feature, where EPCDS informs resources, every time EPCIS address is given to any authorized user.

7.3. Client Application

Current functions in EPCDS of SecDS model are mainly implemented as services. As a result, users need to implement their own systems to query EPCIS resources and aggregate the results. In order to reduce complexity for users, it would be good to develop a sample secure client application which stores EPCIS addresses, queries to EPCIS resources and aggregate the results efficiently. As such, those users, who do not implement their own system, can use this application to get the required EPC event information.

7.4. Load Balancing and Clustering

As mentioned in Section 5.5., SecDS model might have problem of supporting increased number of user queries and EPCIS resources. To solve this problem of scalability, load balancing and clustering techniques can be considered. Clustering a few servers when load-balancing between them can increase the efficiency of access control policy processing. However, co-currency control should be taken care of when there is more than one running server.

7.5. Other Security Measures

EPCDS is considered as trusted and reliable agent between user and EPCIS resources. To use EPCDS in practical business world, there are many security measures to

be considered and implemented.

7.5.1. Authentication

Current SecDS model does not implement any public key based authentication schemas for users and resources. In reality, there should be a certificate authority which can verify the authenticity of publishing and querying companies and their roles in supply chain.

7.5.2. Integrity

To ensure integrity of the messages communicated, every message should be signed with the private keys of the sender.

7.5.3. Availability

Denial-of-service attacks should also be prevented by limiting the number of queries for each user and publisher.

8. Future Direction of EPCDS

In the future, it is expected that EPCDS will be used for "Internet of Things (IOT)" [7]. IOT is a network of physical objects, expected to be implemented in near future. In IOT, most physical objects in the world will have RFID or barcode tags and become uniquely identifiable and connected to the Internet via RFID, sensor, and network technology. Either they are moving in certain directions or standing still in specific places, the physical objects will be tracked by respective owners and that information may be shared with relevant individuals, business partners or even the public. In IOT, EPCDS will play a critical role as a search engine, like Google in the current Internet.

9. Acknowledgements

This work is partly supported by A*Star SERC under grant number 082 101 0022 in Singapore.

REFERENCES

- [1] Wikipedia, "Supply Chain," 2011. http://en.wikipedia.org/wiki/Supply_chain
- [2] Wikipedia, "Bullwhip Effect," 2011. http://en.wikipedia.org/wiki/Bullwhip_effect
- [3] Wikipedia, "EPCglobal," 2010. <http://en.wikipedia.org/wiki/EPCglobal>
- [4] Wikipedia, "Electronic Product Code," 2011. http://en.wikipedia.org/wiki/Electronic_Product_Code
- [5] Wikipedia, "EPCglobal Network," 2010. http://en.wikipedia.org/wiki/EPCglobal_Network
- [6] EPCGlobal, "The EPCglobal Architecture Framework," 2010. <http://www.gs1.org/gsm/kc/epcglobal/architecture/archit>

- ecture_1_4-framework-20101215.pdf
- [7] Wikipedia, "Internet of Things," 2012. http://en.wikipedia.org/wiki/Internet_of_Things
- [8] University of Cambridge, AT4 Wireless, BT Research, SAP Research (BRIDGE project), "High Level Design for Discovery Services," 15 August 2007. <http://www.bridge-project.eu/data/File/BRIDGE%20WP02%20High%20level%20design%20Discovery%20Service%20s.pdf>
- [9] J. Muller, J. Oberst, S. Wehrmeyer, J. Witt, A. Zeier and H. Plattner, "An Aggregating Discovery Service for the EPCglobal Network," *Proceedings of the 43rd Hawaii International Conference on System Sciences*, Hawaii, 5-8 January 2010, pp. 1-9.
- [10] S. Jie, D. Sim and L. Yingjiu, "SecDS: A Secure EPC Discovery Services System in EPCglobal Network," *2nd ACM Conference on Data and Application Security and Privacy (CODASPY)*, San Antonio, 7-9 February 2012, pp. 267-274.
- [11] C. Kürschner, C. Condea, O. Kasten and F. Thiesse, "Discovery Service Design in the EPCglobal Network: Towards Full Supply Chain Visibility," *Proceedings of the 1st International Conference on the Internet of Things*, Zurich, 26-28 March 2008, pp. 19-34.
- [12] E. Polytarchos, S. Eliakis, D. Bochtis and K. Pramataris, "Evaluating Discovery Services Architectures in the Context of the Internet of Things," *Unique Radio Innovation for the 21st Century*, Part 3, 2010, pp. 203-227.
- [13] E. Sergei, F. Benjamin, K. Steffen and S. Nina, "Comparison of Discovery Service Architectures for the Internet of Things," *Proceedings of the 2010 IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing*, Newport Beach, 7-9 June 2010, pp. 237-244. [doi:10.1109/SUTC.2010.22](https://doi.org/10.1109/SUTC.2010.22)
- [14] Afiliat, "Finding Your Way in the Internet of Things," 2008. http://www.afiliat.info/webfm_send/11
- [15] K. Framling, M. Harrison and J. Brusey, "Globally Unique Product Identifiers—Requirements and Solutions to Product Lifecycle Management," *Proceedings of 12th IFAC Symposium on Information Control Problems in Manufacturing (INCOM)*, Ecole des Mines, Saint Etienne, 17-19 May 2006, pp. 17-19.
- [16] B. Fabian, "Implementing Secure P2P-ONS," *Proceedings IEEE International Conference on Communications*, Dresden, 14-18 June 2009, pp. 988-992.
- [17] ISO, "Software Engineering—Product Quality—Part 1: Quality Model," 2001. ISO/IEC TR 9126-1:2001