一种带权限管理的 EPC IS 设计方案①

梁 洁

(武汉理工大学 计算机科学与技术学院, 武汉 430063)

摘 要: EPC IS 在物联网中处于核心地位, 它担负着对大量 EPC 数据和 PML 文件的处理解析任务. 在传统的 EPC IS 的基础上, 结合可扩展的访问控制高标识语言(XACML), 提出了一种带权限管理的 EPC IS 设计方案, 以解决企业之间互相访问 EPC IS 所带来的一系列安全问题. 首先介绍了传统的 EPC IS 的架构和作用以及所带来的安全隐患, 然后引入了 XACML, 重点分析如何实现权限管理, 最后针对跨企业的供应链管理系统给出一个带权限管理的 EPC IS 设计方案.

关键词: 权限管理; EPC 信息服务; 实体标记语言; 可扩展的访问控制高标识语言; EPC IS 设计方案; 供应链管理系统

EPC IS Design Schema of Rights Management

LIANG Jie

(School of Computer Science and Technology, Wuhan University of Technology, Wuhan 430063, China)

Abstract: The EPC IS is the core of the Internet of Things and it's responsible for the tasks of analyzing EPC datas and PML documents. Thus, this paper discusses a new EPC IS design scheme of Rights Management based on the traditional EPC IS while combined with eXtensible Access Control Markup Language (XACML). This new EPC IS design scheme of Rights Management aims to resolve the security issues of the EPC IS when it is accessed across companies. The architecture and role of the EPC IS with potential security problems come first. Then, XACML, which focus on analyzing how to realize rights management is talked. Finally, an EPC IS design schema of rights management solution of the cross-enterprise supply chain management system is put forward.

Key words: rights management; EPC IS; PML; XACML;EPC IS design;supply chain management

随着物联网技术的发展, 物联网的应用也越来越广泛, 在交通、物流、医疗、农业等方面的应用已突显物联网技术的优势. 由于物联网中涉及到大量的实体, 处于物联网的核心地位的 EPC IS(Electronic Product Code Information Service: EPC 信息服务)担负着对大量交互信息的处理, 所以 EPC IS 设计的好坏影响到整个物联网信息交互的效率. 而物联网中处于管理角色的各个企业都有各自的 EPC IS, 在 EPC IS 中存储着 EPC 的相关事件和所对应的实体的商业扩展信息, 以及本企业的相关管理信息, 通过对本企业或其他企业的 EPC IS 的访问, 来实现对实体或产品的完整信息的查询和管理. 但同时也带来一个问题, 如何设计跨企业的 EPC IS, 以实现对数据的有效管理和安全访问. 因为 EPC IS 中必然保存有本企业的商业秘密等相关信息, 这样各个企业的相互访问就会带来一系列的安全问题, 所以应该引入权限管理机制, 使得对不同的企业的访问请求进行权限控制. 本文基于这个研究方向, 引入 XACML (eXtensible Access Control Markup Language: 可扩展的访问控制高标识语言)实现权限管理机制, 针对跨企业的供应链管理系统提出了一种带权限管理的 EPC IS 的设计方案.

① 收稿时间:2012-01-09;收到修改稿时间:2012-02-29

1 EPC IS

1.1 EPC IS 在 EPC 系统中的作用

在物联网中, 对于实体的信息交互, 首先建立EPC(Electronic Product Code: 产品电子代码)编码标准以建立全球通用的信息交换语言. EPC 是一种能够唯一标识所有实体的技术[1]. 通过在被识别实体上装载带有 EPC 的电子标签, 将标签中存储的 EPC 匹配到相应的 EPC IS 上, 对发送过来的数据进行存储、解析以及读出. 信息以两种方式存储, 一是存储在数据库中, 二是存储在 PML 文件中. PML(Physical Markup Language: 实体标记语言)[2]是用来提供一种通用的标准化的词汇来表示实体对象、过程和环境, 它是 EPC 系统中的通信语言, 也是一种数据保存方式, 可实现在不同的环境下的无障碍的通信.

EPC IS 在整个 EPC 网络中处于服务器的地位, 其设计是为了减少电子标签的存储容量以降低电子标签的成本, 使得在电子标签内只存储 EPC, 余下的相关数据信息存贮在 EPC IS 中, 并通过 EPC 来实现对产品信息的维护和更新.

1.2 传统的 EPC IS 架构

传统的 EPC IS 架构如图 1 所示.

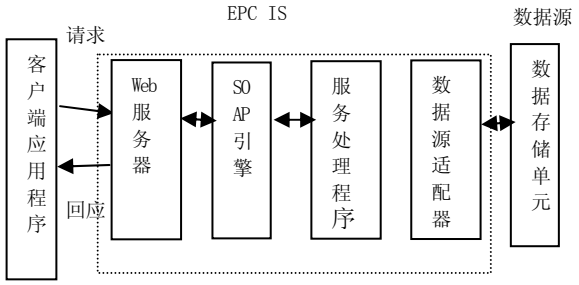

图 1　传统的 EPC IS 整体架构

EPC IS 是一个典型的 Web 服务, 其上层接口接收到客户端以 PML 格式发送过来的数据信息, 根据客户端的请求, 通过 SOAP 引擎将请求对应到特定的服务处理程序上, 服务处理程序对 PML 进行解析, 并根据操作和解析结果维护更新 EPC IS 上保存的相应的产品信息, 最后将结果返回.

但是在实践中, 对企业 EPC IS 中存储的 EPC 相关信息的访问必然会涉及到企业的商业机密和内部管理信息的访问, 而且不同的企业所扮演的角色应该是不一样的, 这样造成不同的企业可以访问的信息也是不一样的. 因此, 必须在传统的 EPC IS 中引入权限管理机制, 使得在一定的授权范围内合理、安全的访问.

2 权限管理机制的引入

2.1 权限管理的需求说明

供应链管理系统主要涉及到三个功能, 即“产品基础信息管理”、“产品定位跟踪管理”以及“库存管理”, 相对应的数据访问操作有数据存储、查询和更新. 而各个处于供应链上的原料供应商、产品生产商和零售商, 本地的 EPC IS 上保存着本企业的产品信息, 同时也可以访问异地的 EPC IS 以整合出产品流通情况, 但是由于一个企业的 EPC IS 中保存着本企业的商业信息和行业机密, 各个企业对 EPC IS 的相互访问也就带来了一系列信息安全方面的隐患. 所以在实践中, 针对跨企业的 EPC IS 的访问权限应该是不相同的, 应该引入权限管理机制.

2.2 XACML

2.2.1 XACML 概述

XACML 是 OASIS(结构化信息标准促进组织)制定的一种可扩展的访问控制标记语言规范, 用于描述应用系统的访问控制策略以及访问控制决策请求、响应信息[3]. 它主要是用来创建一种标准的、可移植的方法来描述访问控制实体和属性, 并提供一种更粒度的控制访问方式.

XACML 包含一个或多个策略(Policy). 策略是基于 XACML 访问控制框架中最小的交互单元, 它由策略管理点产生并维护, 策略有 4 个部分, 即目标(Target)、组合算法、规则集(Rules)和职责集[4].

2.2.2 XACML 体系结构

XACML 的体系结构由 PAP(Policy administration point,: 策略管理点)、PIP(Policy information point: 策略信息点)、PDP(Policy decision point, 策略决策点)、PEP(Policy enforcement point, 策略执行点)构成[5]. XACML 的权限管理流程如图 3 所示, 首先授权请求到达 PEP, PEP 将此请求转换成 XACML 标准请求发送给 PDP, 由 PDP 访问 PAP 编写的策略或者调用由 PIP 搜索到的与主体、资源、环境相关的属性值来判断请求是否符合授权决策并返回响应.

2.3 引入了权限管理机制的 EPC IS

XACML 符合 XML 规范, 具备可扩展性, 具有很强的访问控制策略描述能力, 将 XACML 机制引入 EPC IS 的设计中, 能在不改变 EPC IS 上层数据接口的

情况下, 用户权限验证模块能与上层数据接口无缝连接. 在传统的 EPC IS 上增加权限管理模块, 引入了权限管理机制的 EPC IS 的整体架构如图 3 所示, 接收由 SOAP 处理后的请求信息, 经该权限验证后, 再发送到对应的服务处理程序中.

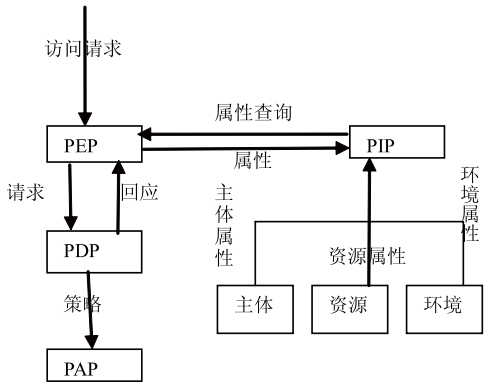

图 2 XACML 权限管理流程

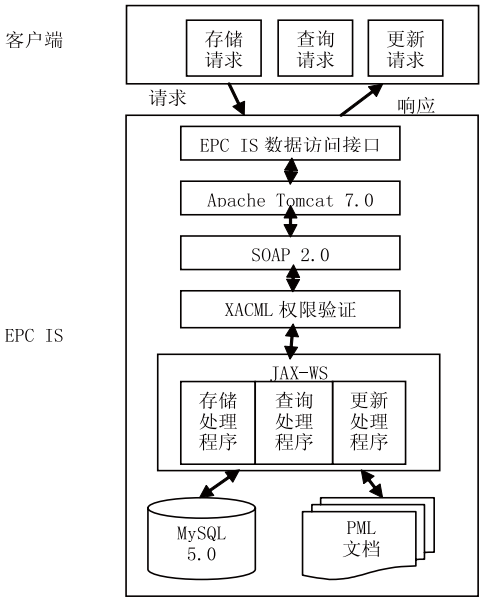

图 3 引入权限管理机制的 EPC IS 整体架构

3 用户权限验证设计

3.1 模块设计划分

用户权限验证分为三个部分: 用户信息存储, 用户授权和权限验证.

首先用户授权模块根据用户的身份(包括企业内部员工, 企业合作关系, 系统管理员等)分配用户权限信息, 将此用户权限信息存储在用户信息存储模块中. 用户信息存储模块分两种方式存储信息, 第一是将用户的用户名、密码和存储用户权限的 XACML 文档路径等用户信息存储在数据库中, 第二是将用户权限具体信息存储在 XACML 文档中. 当用户访问该 EPC IS 时, 权限验证模块将根据从客户端发送过来的用户名和密码等参数查询数据库, 是否有此用户并且用户名和密码正确. 如果正确则说明此用户有权限访问该 EPC IS, 并且返回存储该用户权限的 XACML 文档路径, 当用户提出具体的操作请求的时候, 权限验证模块要查询该 XACML 文档核实该用户是否有此操作的权限.

3.2 权限设计实例

由于 EPC IS 的用户有不同的角色, 现对用户名为 PartnerA@eecc.com 的主体进行决策权限设计, 该主体只具有部分查询的权限, 即只能查询存有包括产品生产日期、产地等等部分信息的资源,例如可以访问 file:///F:/Enterprise/ProductPart1.xml, 而产品的成本等信息是不允许查询到的, 例不能访问 file:///F:/Enterprise/ProductPart2.xml. 由于策略的范围应该比请求的范围广, 可是这样创建两个策略: 具备 eecc.com 电子邮件名的所有用户可以对 file:///F:/Enterprise/ProductPart1.xml 执行“OPEN(打开)”操作, 不能对 file:///F:/Enterprise/ProductPart2.xml 执行任何操作. 在 XACML 中, 规则用资源(Resource)、主体(Subject)、动作(Actions)来描述. 将用户对应于 Subject 的子元素 AttributeValue 的 DataType 属性, 将用户的操作对应于 Action 中, Rule 的 Effect 属性说明操作是否允许. 这样, 可以如下设计决策权限文档, 并将此权限文件存入 Authority.xml 文件.

```
<PolicySet PolicySetId="01">
<Policy PolicyId="1">
<Rule RuleId="PartnerARule1" Effect="Permit">
<Target>
<Subject>
<AttributeValue>eecc.com</AttributeValue>
</Subject>
<Resources>
<AttributeValue>file:///F:/Enterprise/Products/Produ
ctPart1.xml</AttributeValue>
</Resources>
<Actions>
<AttributeValue>OPEN</AttributeValue>
</Actions>
```

```
</Target>
</Rule>
</Policy>
<Policy PolicyId="2">
<Rule RuleId= "PartnerARule2" Effect="Deny">
<Target>
<Subject>
<AttributeValue>eecc.com</AttributeValue>
</Subject>
<Resources>
<AttributeValue>file:///F:/Enterprise/Products/ProductPart2.xml</AttributeValue>
</Resources>
<Actions>
<AttributeValue><AnyAction/></AttributeValue>
</Actions>
</Target>
</Rule>
</Policy>
</PolicySet>
```

4 数据源的设计

由于在 EPC 系统中, 数据来源分为两类: 时标数据和静态属性数据. 时标数据是指从标签读取到的或者是商业交易数据, 是动态数据; 静态属性数据书指定义在单个产品上的属性或是定义在产品级上的属性数据[6]. 时标数据一般保存在数据库中, 而静态属性数据常以 PML 格式的文件保存.

4.1 数据库的设计

使用关系数据库保存时标数据和部分静态数据, 对应的主要的关系模式如下所述:

①“PML 存储”实体型所对应的关系模式: PMLStorage (EPC,PMLpath)

②“产品信息”实体型所对应的关系模式: Products(ProductsID,EPCSeries,TotalNum,SaleNum,StorageLocation,StorageNum,Cost,Price)

③“产品跟踪”实体型所对应的关系模式: ProdutTrace (TraceID,ReaderID,EPC)

④“识读器”实体型所对应的关系模式: Reader(ReaderID,ReaderName,ReaderLocation)

⑤“用户”实体型所对应的关系模式: User(UserID,Password,UserName,AuthorityPath)

进而可以根据这些关系模式在数据库中建立表.

4.2 PML 的设计

在 EPC 网络中的信息交换中, EPC IS 接收到的是以 PML 格式表示的数据, 又以 PML 格式回应各种请求. 按照 PML1.0 的设计标准, 可对一个保存产品名称等信息的 PML 文件的 Schema(模式)做如下所示的设计, ProductPart1.xml 对应于该模式.

```
<xs:schema
xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:pml="http://web.mit.edu/mecheng/pml">
<xs:simpleType name="entity_type">
<xs:sequence>
<!--产品信息-->
<xs:element name="产品名称" type="xs:string"/>
<xs:element name="产品位置" type="pml:location"/>
...
</xs:sequence>
</xs:simpleType>
<xs:simpleType name="product_type1">
<xs:sequence>
<xs:element name="epc 编号" type="xs:string"/>
<xs:element name="entity" type="entity_type"/>
</xs:sequence>
</xs:simpleType>
<xs:element name="product" type="product_type1"/>
</xs:schema>
```

5 应用范例与实现

本设计采用 Apache Tomcat 7.0 作为 Web 服务器监听客户端请求, SOAP 2.0 为 SOAP 引擎作为客户端/服务器端的通讯协议, 引入 XACML 权限管理机制构建权限验证模块, 并采用 MySQL 5.0 作为数据库, 在 MyEclipse 8.0 中使用 JAX-WS 2.0 框架以方便构建和发布 Web 服务来构建 EPC IS.

5.1 应用范例

在这里以销售牛奶的供应链系统为例, 在这条供应链中有三个节点, 分别为牛奶的生产商、批发商和零售商, 这三个节点分表代表了实际的一条简单完备的供应链, 同时这三个企业都拥有各自的 EPC IS.

在实践中, 如果零售商需要查询牛奶的相关信息,

例如产品营养成分等, 则需要访问生产商的 EPC IS. 当用户登录到该服务上时, 首先应该对其权限进行验证. 根据客户端发送过来的用户名和密码, 核对是否有权限登录, 同时返回该用户的 XACML 文档路径, 找到对应的 XACML 文档. 根据已经建立好的 XACML 对该用户进行授权, 确定该用户可访问的范围和操作限制. 如之前已经讨论过的权限实例设计, 该用户只能访问 file:///F:/Enterprise/ProductPart1.xml, 不能访问 file:///F:/Enterprise/ProductPart2.xml, 现对该权限管理机制进行实现.

5.2 依据 EPC 查询产品信息权限管理的实现

在用户进行查询操作之前, 首先应加入决策文件 Authority.xml:

FilePolicyModule filePolicy =new FilePolicy Module();

filePolicy.addpolicy("./Authority.xml");

再将请求以格式化保存到 Requst.xml 中:

RequestCtx request=RequestCtx.getInstance(new FileInputStream ("./Request.xml"));

ResponseCtx response=pdp.evaluate(request);

然后需在数据库中根据 EPC 查询此产品对应的 PML 文档存储路径: String sql="select PMLpath from PMLStorage where EPC =?"; 查询到 EPC 对应的 PML 的存储路径后, 再对此 PML 文档进行解析和遍历, 最后将数据整合反馈给客户端. 由于 PML 符合 XML 的文档规范, 现选择 DOM4J 对 PML 进行解析.

建立此功能的 web 服务, 如下:

@javax.jws.WebService(targetNamespace="http://ws.EPCPML.com/",serviceName="IqPMLService",portName="IqPMLPort",wsdlLocation="WEB-INF/wsdl/IqPMLService.wsdl")

public class IqPMLDelegate {

com.EPCPML.ws.IqPML iqPML = new com.EPCPML.ws.IqPML();

public Product IQByEPC(String epc) {return iqPML.IQByEPC(epc);}

}

最后验证其是否有权限执行相应操作.

5.3 应用结果演示

使用 MyEclipse 8.0 建立 Web Service Client(Web 服务客户端), 通过局域网中访问该 EPC IS, 用户 PartnerA@eecc.com 进行“依据 EPC 查询产品信息”的操作, 演示结果如图 4 所示.

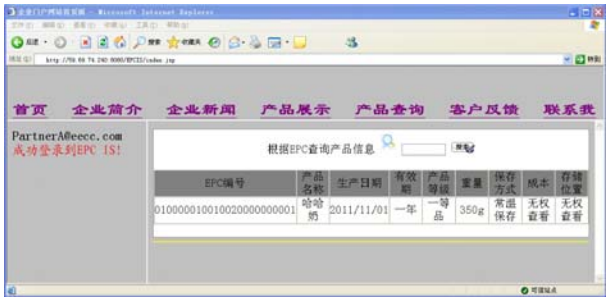

图 4 权限管理结果演示

从演示结果图中可以看到, 该用户无权查看产品的成本和存储位置信息, 实现了权限管理.

6 总结

将物联网技术引入实际的供应链管理系统中, 在各个企业中建立 EPC IS 能方便的对产品的库存和流通情况进行管理. 本文的 EPC IS 的设计方案能满足不同的企业之间对产品管理和安全访问, 使 EPC IS 真正建立在一个可信环境中. 当然, 该设计方案仍然需要进一步的完善, 例如访问的效率问题, 怎样实现异步访问等等, 这些会在以后的工作中进一步研究.

参考文献

1 Brock DL. Integrating the Electronic Product Code (EPC) and the Global Trade Item Number (GTIN). MIT AUTO-ID White Paper. 2001,11(1):4–5.

2 Brock DL, Milne TP, Kang YY. The Physical Markup Language Core Components: Time and Place. MIT AUTO-ID White Paper, 2001,6(1):2–4.

3 彭军,徐燕,高阳.基于 XML 和 XACML 的角色访问控制的实施.石河子大学学报(自然科学版),2005,23(2):252–255.

4 马恒太.Web 服务安全.北京:电子工业出版社,2007.

5 孙建华,巴特尔,王平泉,石利梅.基于 XACML 的 Web 服务访问控制研究.计算机安全,2009,5:64–66.

6 Harrison M. EPCTM Information Service-Data Model and Queries. MIT AUTO-ID White Paper, 2003,10(1):5–7.