协同设计环境中数据库安全共享关键技术研究*)

郎 波 张 鑫 李伟琴
(北京航空航天大学计算机学院 北京 100083)

摘 要 在支持航空产品研制的协同设计平台中,满足设计数据库共享模式的平台架构与安全控制结构是两项关键技术。本文在分析设计数据库特殊的管理与共享模式的基础上,提出了基于CORBA的协同设计平台结构,以及基于数据库访问网关的安全控制方法。在数据库访问网关核心技术的研究中,提出了利用CORBA拦截机制保证数据库网关有效性的方法,为增强型安全产品开发提供了一种新思路。本文最后给出了系统实现与性能测试结果。

关键词 协同设计,CORBA,访问控制,数据库访问网关

Research of Key Technologies of the Secure Database Sharing in Collaborative Design Environments

LANG Bo ZHANG Xin LI Wei-Qin
(School of Computer Science and Engineering, Beihang University, Beijing 100083)

Abstract In building a collaborative platform supporting aeronautics product design, the architecture of the platform which satisfies the design databases sharing mode and the security control method are the two key technologies. On the base of analyzing the special management and sharing mode of the design databases, the paper submits the architecture of the collaborative design platform by using CORBA technology and also submits a kind of database access gateway to achieve the security control of the sharing data. In the research of the key technology of the database access gateway, the paper puts forward a method to ensure the effectiveness of the database access gateway based on the CORBA portable interceptor mechanism, which provides a new thoughts for enhanced security product development. The paper also presents the system implement result and efficiency testing result.

Keywords Collaborative design, CORBA, Access control, Database access gateway

1 概述

在航空型号产品的研制中,由于这种产品规模庞大,因此需要多个航空研究所和企业共同参加设计与制造,而一个研究所内部也有多个设计室参与。每个研究所与研究所内的设计室都建立了相关数据库,设计数据库保存了设计文件的基本信息。研究所和企业之间以及研究所内部各个设计室之间在进行异地协同设计时,需要频繁交换和共享设计数据库中的数据。

航空产品型号设计的数据共享与协同设计有如下特点:(1)研究所与企业之间以及研究所内部各设计室之间数据库一般是单独管理控制,独立性强。(2)协同设计中交换的数据保密性强。由于航空产品研制数据属于保密性很强的数据,这种设计数据的交流需要保证数据的安全。这种安全包括:保证数据不被冒名的用户盗用;传输过程中不被窃取、非法修改;数据库访问进行统一控制,各单位为了实现数据的统一管理、保证数据的安全性与一致性,不希望外界用户直接对数据库进行访问,希望设立统一控制机制;能够实行多种安全策略,即对于本单位内部、上级主管部门、合作单位应该制定不同强度的安全策略,才能既支持协作又有效保证数据的安全。

目前参与航空型号产品研制的研究所和企业都通过航空专网连接起来,但由于缺乏满足型号协同设计特殊需求的协同工作平台,使设计数据的交换与共享大都采用异步手工方式,工作效率比较低。因此,建立航空产品型号研制中符合设计数据管理与共享模式并具有有效安全保证的协同设计平台,对于提高型号研制的工作效率,促进航空事业信息化进程具有重要意义。

本文设计并实现了一种支持航空产品型号研制的数据库共享平台。该平台支持协同设计的研究所与企业的设计数据库共享,并具有数据的安全保护功能。本文将在第2节介绍所提出的数据库安全共享平台的体系结构,在第3节与第4节论述该平台中基于数据库访问网关的安全控制思想与实现方法。最后对本文进行总结与展望。

2 数据库安全共享平台的体系结构

建立航空型号研制协同设计平台的关键在于:(1)符合设计数据的管理控制模式。协同设计平台的管理与控制模式应该符合目前设计数据的管理控制模式,即是在研究所及其设计室、企业独立管理的基础上的有计划、合理的数据共享与交换模式。(2)保证设计数据的安全。虽然目前商品化数据库系统提供一定的安全功能(一般主要是自主型访问控制、密码存储等),但现有数据库的安全功能无法满足航空产品型号协同设计中数据很高的安全性要求。(3)可以与多种产品设计软件或PDM产品数据管理系统有机融合。目前很多研究所和航空制造企业的设计和制造中都采用了PDM系统实现单位内部的产品数据管理,协同设计平台应该能够和这些系统有机融合,访问现有数据库或利用PDM系统的API,通过PDM系统共享设计数据。

*)国家自然基金资助项目(项目编号:60203026),航空基金资助项目(项目编号:02F51064)。郎 波 博士,副教授。

基于上述因素，我们采用 CORBA 作为构建数据库共享平台的主要技术。CORBA 易于实现已有应用系统的集成，并支持局部数据库的独立管理与控制模式[1]。我们进一步研究了在 CORBA 环境中融合安全控制技术的方法，提出了数据库安全共享平台的总体结构，如图 1 所示。

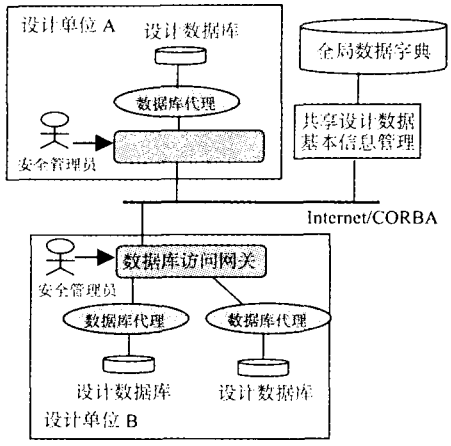

图 1　数据库安全共享平台体系结构图

在图 1 的结构中，建立了共享数据基本信息全局数据字典，并由共享数据基本信息集中管理模块对其进行管理。系统中所有共享数据的基本信息都记录在全局数据字典中。协同系统中的用户通过集中管理模块从全局数据字典中获取所需数据的信息，继而对所需的信息发出访问。协同设计中的用户将通过数据库代理获取相应数据库中的数据。数据库共享中的安全是通过数据库访问网关实现的，它对数据库代理的访问进行控制，具有身份认证、访问控制、数据加密/解密、安全审计等功能，使各个单位可以在有效保护、控制自身数据库的前提下实现数据共享。

数据库安全共享平台主要包括两大部分：

(1)*基于 CORBA 的设计数据共享平台*　在基于航空专网的协同设计平台中，各单位使用的计算机、操作系统、甚至数据库系统都可能不同，是异构性非常强的环境，引入 CORBA 能够屏蔽异构性。另外利用 CORBA 机制的面向对象的特征，对各个数据库能够实现封装，对外提供统一的接口，实现各数据库在互操作前提下的独立管理与控制。

基于 CORBA 的协同设计平台的基本思想是：对各个设计数据库进行封装，形成 CORBA 中的服务对象，称为数据库互操作的代理，即数据库代理。数据库代理实现各个数据库之间数据交换所需要的数据操作。

(2)*数据库共享中的安全控制*　协同数据共享平台中的安全是通过建立数据库访问网关实现的。该网关可以进行用户身份认证，并依据本单位制定的安全策略实现对数据库代理的控制，另外还对协同平台中传输的共享数据进行加密。

数据库共享的安全控制是协同设计平台的关键。

3　基于数据库访问网关的安全控制方法

数据库访问网关是协同设计平台实现数据安全互操作的关键。它位于系统中数据库互操作的逻辑路径上，对任何一个数据库的访问操作都必须经过数据库访问网关的控制。每个单位可以建立一个或多个数据库访问网关，独立配置安全策略实现对本单位数据库中共享数据的安全控制。数据库访问网关可以实现数据的加密/解密、访问请求者的身份认证、访问控制以及安全审计等功能。数据库访问网关的结构如图 2 所示。

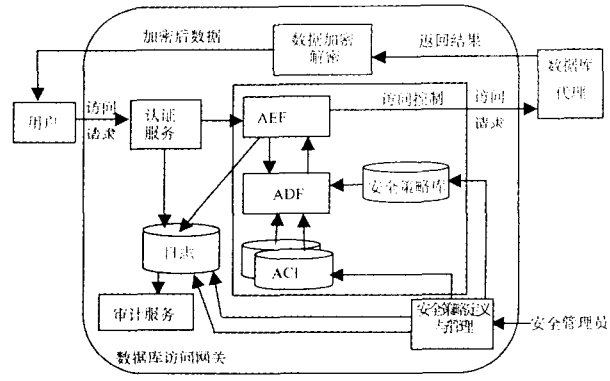

图 2　数据库访问网关的结构

3.1　访问控制机制

数据库访问网关中的访问控制机制由访问控制验证机制 ADF(Access control Decision Function)、访问控制执行机制 AEF(Access control Enforcement Function)、访问控制信息 ACI(Access Control Information)以及安全策略库等组成[2]。访问控制过程是：用户经过数据库访问网关的认证后，用户的操作请求首先被 AEF 拦截，AEF 接着向 ADF 提出验证请求，ADF 根据安全策略库中定义的安全策略对 AEF 的请求做出“允许”或“拒绝”的决定。AEF 在接收到 ADF 的决策结果后，进一步执行该结果。如果 ADF 返回的是“允许”，则 AEF 将根据用户请求的操作激活相应的数据库代理，并把操作的结果返回给用户；否则 AEF 将把“拒绝”访问的信息直接返回给用户。

为了支持共享数据根据不同请求采取不同安全策略，ADF 实现了动态支持多策略的柔性化访问控制。关于这方面研究可参见文[3]。

3.2　安全策略定义与管理

安全策略定义与管理，使安全管理员定义系统安全策略。所定义的安全策略信息将记录在访问控制的安全策略库中，作为数据库访问网关进行安全策略验证的依据。另外安全管理员可以通过该模块对访问控制信息 ACI 进行配置。

3.3　其它安全服务

用户的身份认证、数据加密、审计等安全服务是计算机安全中的基本服务。数据库访问网关通过采用插件式的开放体系结构，除了对用户请求进行访问控制以外，还可以集成用户的身份认证、数据加密/解密、审计等安全服务。访问控制与认证服务、数据加密/解密、审计服务作为不同的插件既相互联系又相互独立，可以分别实现并通过插件接口联结起来。因此，对于认证服务可以采用多种成熟的技术，如基于 PKI 的身份认证或一次性口令等技术。

上述基于 CORBA 的分布式数据库安全互操作的体系结构，以 CORBA 提供的分布式对象互操作模型为基础，设计了系统安全控制与互操作机制，既保证了各个局部数据库的安全与自治，又实现了数据的共享与互操作。

4　数据库访问网关的实现方法

设计与实现数据库访问网关的关键是如何保证它的不可旁路性即有效性，使得外界对某个局部数据库的访问不能绕过数据库访问网关进行。本文提出利用 CORBA 本身的互操

作机制将网关与 CORBA 软件融合，以保证其有效性。该研究属于增强型安全技术研究。通过这种增强型安全技术，能够把具有自主知识产权的安全产品融合到国外先进的 CORBA 软件中，所形成的增强型安全软件能够快速、直接地应用到国民经济建设的实际应用中，显著提高这些系统的安全保护能力。

本文提出利用 CORBA 的拦截机制，实现数据库访问网关的不可旁路性。

4.1 CORBA 的可移植拦截器

CORBA 框架中的 ORB(Object Request Broker)是实现客户端和服务对象之间互操作的核心组件。ORB 实现客户端和服务对象之间消息传递的过程是相对封闭的，基于 CORBA 的应用系统一般无法对 ORB 的处理过程进行干预。而在某些应用环境中，需要使 ORB 在处理过程中执行一些特殊控制(称为 ORB 服务)，如服务对象的安全控制、事务处理等。能够使 ORB 实现这种操作的方法有两种：一种是修改 ORB 的实现，但这种方法不具有通用性。另一种方法是利用 CORBA 提供的 ORB 拦截器(Interceptor)机制，将 ORB 服务封装为一个拦截器嵌入到 ORB 中，则 ORB 在处理客户端与服务对象之间交互时，就会在某些预定时刻执行拦截器，从而实现某些特殊控制功能。这种拦截器能够保证与 ORB 的相对独立，使作为拦截器的 ORB 服务可以在不同的 ORB 上运行，具有可移植性，所以被称为可移植拦截器(Portable Interceptor)[1,4]。利用可移植拦截器还可以实现 ORB 监控、安全应用、负载均衡等其它复杂服务[5]。

CORBA 规范中定义了两种类型的拦截器，IOR(Interoperable Object References，可互操作对象引用)拦截器和请求(Request)拦截器。IOR 拦截器适用于可互操作对象引用的创建过程的处理，可以在创建对象引用的过程中加入 ORB 服务特有的标记组件。请求拦截器适用于拦截请求处理的过程。请求拦截器可分为两种：客户端请求拦截器和服务器端请求拦截器。客户端请求拦截器用于对客户端操作的拦截，包括客户端发送请求，和接收服务器端返回信息两个过程。服务器端请求拦截器可以获取客户端请求拦截器增加的附加信息以及操作请求相关信息，并可以对服务对象返回的操作结果进行处理。

4.2 数据库访问网关嵌入机制设计

对上述拦截器机制的分析表明，完全可以利用这种拦截机制，将数据库访问网关作为拦截器插入到 CORBA 的 ORB 核心中，解决其不可旁路性问题。

为 ORB 添加访问控制拦截器的步骤如下[1,6]：

(1) 将数据库访问网关封装为拦截器。一般将数据库访问网关作为服务器端请求拦截器。

(2) 构造 ORB 初始化器，将定义好的数据库访问网关拦截器与 ORB 初始化器绑定。

(3) 将 ORB 初始化器注册到 ORB 中。

数据库访问网关拦截器可以通过 ORB 初始器添加到多个 ORB 中，因而实现了拦截器与具体 ORB 的分离，具有良好的可移植性。

(1) ORB *初始化器的构造*　数据库访问网关要作为 ORB 服务成为 ORB 的一部分，才能使 ORB 在处理过程中自动执行。因此数据库访问网关拦截器的注册必须在 ORB 的初始化过程中完成，而不能在一个已经完成初始化的 ORB 上添加。可以通过 ORB 初始化器(ORBInitializer)向 ORB 注册数据库访问网关拦截器。

每个 ORB 在构造时，都可以指定一个 ORB 初始化器。ORBInitializer 的 IDL 定义如下：

```
local interface ORBInitializer {
    void pre_init( in ORBInitInfo info );
    void post_init( in ORBInitInfo info );
};
```

当 ORB 初始化器注册到 ORB 后，ORB 会在初始化的过程中自动调用方法 pri_ init()和 post_ init()来为 ORB 添加需要的拦截器。方法中的输入参数 info 为一个 ORBInitInfo 对象，它表示当前 ORB 的初始化信息。

(2)ORB *初始化器的注册*　ORB 初始化器的注册过程，需要根据编程语言的不同采用不同的方法。在 Java 语言中，可以通过指定 ORB 的属性方法来完成：

```
props. put("org. omg. PortableInterceptor.
        ORBInitializerClass. com. uzi. interceptor. ServerInitializer ",
"");
org. omg. CORBA. ORB orb = org. omg. CORBA. ORB. init ( null ,
props);
```

这样一条语句为 ORB 增加了初始化器 com. uzi. interceptor. ServerInitializer。

4.3 数据库访问网关嵌入机制的实现

数据库访问网关嵌入的具体实现如图 3 所示，图中的服务器端拦截器封装了数据库访问网关。下面以数据库访问网关实现自主访问控制策略 DAC 为例介绍实现过程。

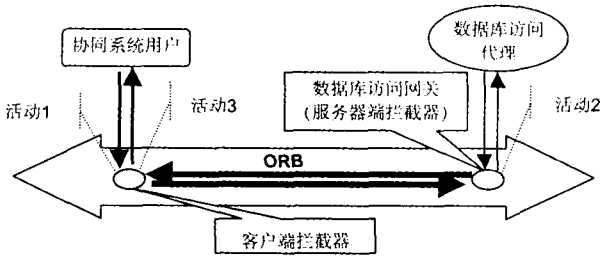

图 3　采用拦截机制的数据库访问代理的安全

ORB 在处理用户与一个 CORBA 对象之间交互的不同时刻，激活了图 3 中的活动 1、活动 2 和活动 3，实现如下处理：

活动 1：当客户向服务器端发送请求时，客户端拦截器截取客户端的输出流，并向流中添加用户的基本信息。

活动 2：数据库访问网关作为服务器端拦截器截取服务器端的输入流，获得客户端添加的用户基本信息，根据用户的基本信息查询 DAC 策略的 ACL(访问控制列表)，判断用户的权限。如果用户越权，则抛出异常，客户端的请求被截断，否则将客户端的输入流提交至 CORBA 服务对象。

活动 3：客户端拦截器在客户端截获服务器端返回的信息，判断服务器端返回信息的类型。如果接收到的服务器返回信息为服务器端拦截器所抛出的异常，则通知客户端对服务器对象的此次请求越权，否则将服务器端的信息继续发送到客户端。

客户端拦截器由 ClientForwardInterceptor 实现。ClientForwardInterceptor 类实现了接口 ClientRequestInterceptor，此接口是客户端请求拦截器的 IDL 定义在 Java 语言的映射。虽然该 IDL 接口中一共定义了 5 个方法，但具体实现的时候，只须根据具体的应用需要，实现其中的一部分方法。ClientForwardInterceptor 实现了其中的方法 send_ request( )和 receive_ exeption( )用于完成图 3 中的任务 1 和任务 3。任务

2 是通过服务器端拦截器实现的，具体的实现类似于上述客户端请求拦截器。

完成 Interceptor 定义后的任务就是服务器端和客户端 ORB 初始器的构造。ORB 初始器的构造，可以通过实现接口 ORBInitializer 来完成。最后将两个 ORB 初始器分别注册到客户端 ORB 和服务器端 ORB 中。上述设计分别在两种 CORBA 平台 Jacorb1.40 和 Orbix2000 上进行了实现。

5 系统实现与测试

将 JSP/JAVA Bean 技术与 CORBA 技术相结合，我们建立了基于 Web 的支持协同设计的数据库安全共享平台，如图 4 所示。

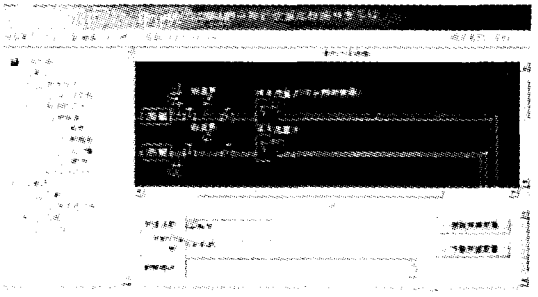

图 4 系统实现结果示例

系统采用了基于 Web 的客户端-应用服务器-数据库服务器的三层体系结构。在应用服务器中利用 JavaBean 作为客户端代理与各个实现共享数据操作的数据库代理交互。协同系统中的用户既可以通过基于 Web 的界面提交共享数据、获取并显示自己有权进行访问的共享数据，还可以通过应用程序编程接口，在应用程序中访问和操作共享数据。

另外，对于数据库安全网关进行了性能测试与分析。测试环境如下：

• 硬件 应用服务器：CPU 1.5Ghz，内存 512M；数据库服务器：CPU 800Mhz，内存 256M。

• 软件 操作系统：Windows 2000 Professional；应用服务器：Tomcat4.1.24；数据库服务器：SQLserver2000；CORBA：JacORB1.4。

选取的测试点是应用服务器中用 JavaBean 封装的 CORBA 客户端获取共享数据所需要的时间。测试中访问的共享数据大小为 100k。分别对三种情况进行测试：(1)共享数据访问中不使用任何安全控制，即不启用数据库访问网关；(2)采用固定的 MAC 策略进行访问控制；(3)采用动态支持多策略的柔性化访问控制；(4)在柔性化访问控制基础上增加了数据加密。表 1 中记录了 6 次测试结果。

表 1 数据库访问网关性能测试数据 （单位：ms）

	1	2	3	4	5	6
无安全控制	515	500	547	515	546	531
MAC 策略	625	656	625	630	657	641
动态访问控制	718	672	719	657	672	703
动态访问控制、加密	859	828	859	828	844	829

测试结果表明，在数据库共享平台中增加数据库访问网关，将增加系统 40%～60%的响应延时，虽然一定程度降低了系统的效率，但也是可接受的。目前正对数据库访问网关的实现进行优化，以提高系统的响应效率。

小结 本文针对航空型号产品异地协同设计中数据库共享的特殊需求，研究并实现了基于 CORBA 的数据库安全共享平台。数据库访问网关的设计与实现，符合协同设计环境中的数据库管理模式，实现了数据共享所需的各种安全技术的有机集成，并且通过利用 CORBA 的可移植拦截器机制，实现了数据访问网关与 CORBA 软件的有机融合，保证了数据库访问网关的有效性。本文在数据库访问网关有效性的研究中，提出了一种增强型安全产品的研究方法。该方法的思想是把具有自主知识产权的安全产品融合到国外先进的安全基础软件中，使增强型安全软件能够快速、直接地应用到国民经济建设的实际应用中，显著提高这些系统的安全保护能力。

参 考 文 献

1 Object Management Group. The common Object Request Broker: Architecture and Specification, Version 2.6, Dec. 2001

2 ISO/IEC 10181-3 Security frameworks for open systems—Access control framework, 1996

3 郎波，吴琦，李伟琴. 分布式对象柔性化访问控制方法研究. 北京航空航天大学学报，30(5)

4 Marchetti C, Verde L, Baldoni R. CORBA Request Portable Interceptors: A Performance Analysis. Conf. On Very Large Data Bases, Santiego, Chile, 1994. 24～35

5 Othman O, O'Ryan C, Schmidt D C. The Design of an Adaptive CORBA Load Balancing Service. IEEE Distributed Systems Online, Apr. 2001.2

6 Brose G, Muller S. JacORB 1.4 Programming Guide Version1.1.9. Mar. 2002, 20

（上接第 225 页）

综合上面所述，可以发现结合消息机制的屏幕共享方法所达到的效果在各个方面都优于其他功能软件，是一种很好的实现屏幕共享的方法。

结束语 屏幕共享技术是一个非常有潜力的应用技术，各种基于屏幕共享技术的软件产品必将在远程教学、监控和多媒体应用中发挥越来越大的作用，从而具有广阔的应用前景和市场前景。该论文旨在解决基于 Windows 操作系统的屏幕同步共享问题。通过对该方案的实施可以达到非常好的同步效果。实现真正的屏幕同步共享。

参 考 文 献

1 陈琦，李凡，朱光喜. 屏幕共享技术及其在多媒体通信中的应用. 华中科技大学电信系图像教研室

2 红蜘蛛软件制作室. Red Spider. http://www.forclass.com

3 徐挺，吉逸，金胜昔，等. 计算机网络技术在远程教学系统中的应用研究. 见：[第十届中国计算机学会网络与数据通信学术会议论文集]. 南京，1998. 335～337

4 王建华，张焕生，侯丽坤. Windows 核心编程. 机械工业出版社

5 张友生. 远程控制编程技术. 电子工业出版社

6 SYMANTEC 公司. PcAnyWhere. http://www.symantec.com/

7 Zahariadis Th, Voliotis S. Networking multimedia classromm initiative. Video/Image Processing and Multimedia Communications 4th EURASIP-IEEE Region 8 International Symposium on VIPromCom 16-19 June 2002. 35～38

8 Pekowsky S, Andorfer A. Multimedia data broadcasting strategies. Communications Magazine. IEEE April 2001, 39(4): 138～145