第33卷 第23期 计 算 机 工 程 2007年12月
Vol.33 No.23 Computer Engineering December 2007
·开发研究与设计技术· 文章编号：1000—3428(2007)23—0267—03 文献标识码：A 中图分类号：TP311.5

数字化校园综合应用软件平台的关键技术

张学旺[1]，汪林林[1]，马中峰[2]
(1. 重庆邮电大学软件学院，重庆 400065；2. 中南大学网络中心，长沙 410045)

摘 要：综合应用软件平台是数字化校园建设的核心内容之一。文章提出了一种基于Web服务的数字化校园综合应用软件平台架构，叙述了数字化校园综合应用软件平台的3种关键技术(校园信息门户、校园PKI/CA和数据集成)的基本原理、设计要点和创新性。实践证明基于上述软件架构和关键技术构建的数字化校园综合应用软件平台运行安全、可靠、用户满意度高。

关键词：数字化校园；校园信息门户；PKI/CA；数据集成；Web服务

Key Technologies of Integration Application Software Platform for Digital Campus

ZHANG Xue-wang[1], WANG Lin-lin[1], MA Zhong-feng[2]
(1. College of Software, Chongqing University of Posts and Telecommunications, Chongqing 400065;
2. Network Center, Central South University, Changsha 410045)

【Abstract】 Integration application software platform is a core component during construction of digital campus. A software architecture based on Web services for digital campus's integration application software platform is introduced in this paper, then fundamental theory, key factors and creativities to design of three key technologies for the digital campus's integration application software platform(campus information portal, PKI/CA, and data integrity)are emphasized. Practice shows that the digital campus's integration application software platform based on above software architecture and the key technologies runs securely, reliably, and gains several universities' praises during its operation.

【Key words】 digital campus; campus information portal; public key infrastructure(PKI)/certificate authority(CA); data integrity; Web services

数字化校园是现代信息化技术与现代教育理念相结合的产物。数字化校园指利用计算机技术、网络通信技术对学校的教学、科研、管理和生活服务等所有信息资源进行全面的数字化，并科学规范地对这些信息资源进行整合和集成，以构成统一的用户管理、资源管理和权限控制；通过组织和业务流程再造，推动学校进行制度创新、管理创新，最终实现教育信息化、决策科学化和管理规范化[1~2]。

数字化校园建设必将带来学校管理体制和管理流程等的变化，向科学化、规范化变化，计算机应用系统不是原有管理流程的自动化。其理念分为2个方面：以提高教育质量和办学效益为中心(以教师和学生为中心)；以教育发展为动力，教育改革为先导，现代教育理论、管理科学理论和信息科学理论为基础，以信息技术推进教育的现代化，实现教育的跨越式发展。因此，数字化校园≠校园网+应用软件+信息资源；正确的理解应该是：数字化校园=*f*(办学理念，人力资源，服务对象，校园网，应用软件，信息资源)，即以办学理念、人力资源、服务对象、校园网、应用软件、信息资源为输入参数的函数综合体。

1 数字化校园综合应用软件平台的架构设计

1.1 数字化校园架构

简单地说，数字化校园架构可以归纳为一个中心、两个基本点、三网合一、四个层次[1~2]。(1)一个中心：数据中心(IDC)；(2)两个基本点：标准，安全；(3)三网合一：数据，语音，视频；(4)四个层次：网络基础层(主要指校园网基础设施)，网络服务层(主要指校园网提供的基本服务)，应用支撑层(主要指各种应用系统)，信息服务层(主要指用户服务界面和门户)。

1.2 数字化校园综合应用软件平台架构设计

本文的软件架构基于Web services，采用Web services技术作为实现的核心技术，信息和服务中心通过Web services向各个应用支撑系统提供服务，并通过门户向用户提供信息和应用的集成。Web services使用标准的互联网协议(如HTTP和XML)，采用面向对象技术包装数据，通过简单对象访问协议(simple object access protocol, SOAP)实现基于Web的不同应用服务和访问，采用Web服务描述语言(Web services description language, WSDL)描述服务，采用统一描述、发现和集成(universal description, discovery and integration, UDDI)发布服务。这种访问过程就是通过WSDL, SOAP和XML技术来远程调用各种发布的服务，Web services实质上是一种分布式结构。

Web services为Web信息系统的集成提供了一种全新的、更加方便有效的方法。当把Web services应用到信息系统集成中时，需要集成的所有系统都成为一个松散结构中的组件，系统接口、应用通信、数据转换和目录信息都是建立在开放

基金项目：重庆市自然科学基金资助项目(CSTC2006BB2369)；重庆市教委科学技术研究项目(KJ050508)
作者简介：张学旺(1974－)，男，讲师、硕士，主研方向：网络信息安全，软件工程；汪林林，教授；马中峰，学士
收稿日期：2007-07-24 **E-mail：**csxwzhang@hotmail.com

的、被广为接受的标准之上，使用户能迅速地访问到他们所需要的信息。另外，因为 Web services 是由一系列标准组成的，所以 Web services 集成各种应用的方法是标准化的，具有较好的通用性和兼容性，同时面向对象和 XML 等技术的采用使得 Web services 具有更好的跨平台性和通用性，能更好地满足分布式集成的要求。

数字化校园综合应用软件平台的架构如图 1 所示[2]。在图 1 中，数据库及其接口是数据的存储中心，其中公有数据库存放公共信息和从各个私有数据库中抽取的可以公开发布的信息，通过公有数据接口由公共信息发布系统发布；而OID则存放用户信息，包括账号、密码、身份、权限和个人信息等，它可以通过公有数据接口和Web服务向所有的实例系统提供身份认证、用户权限和个人信息等内容。每个应用支撑系统一般都有一个私有数据库，存放该系统的数据，并通过私有数据接口发布。私有数据接口实际上是一个SQL的通用封装器，目的是保证数据的安全、完整和访问的效率。

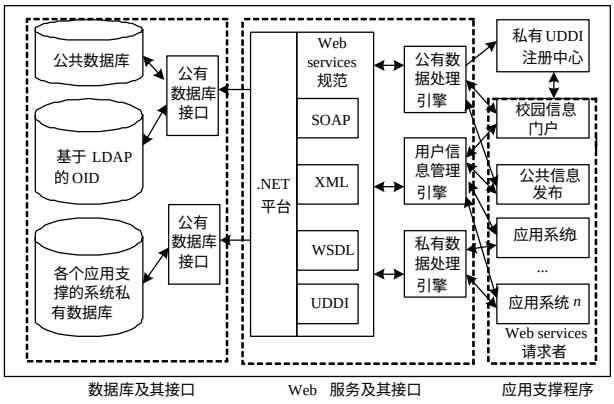

图 1　基于 Web services 的系统架构

Web services 及其接口实际上是一个通过 Web services 形式提供的数据操作功能的集合，通过它应用程序可以按照各自的权限访问相应数据。

所有 Web services 都通过平台私有的 UDDI 注册，各个应用支撑系统可以从 UDDI 获取各个 Web services 的 WSDL 描述，从而利用 WSDL 描述来调用具体的 Web services。

2　数字化校园综合应用软件平台的关键技术设计

数字化校园综合应用软件平台涉及很多技术，本文着重介绍如下 3 种关键技术(校园信息门户技术、PKI/CA 技术和数据集成技术)的基本思想、设计要点和创新性。

2.1　校园信息门户

数字化校园信息门户架构如图 2 所示。

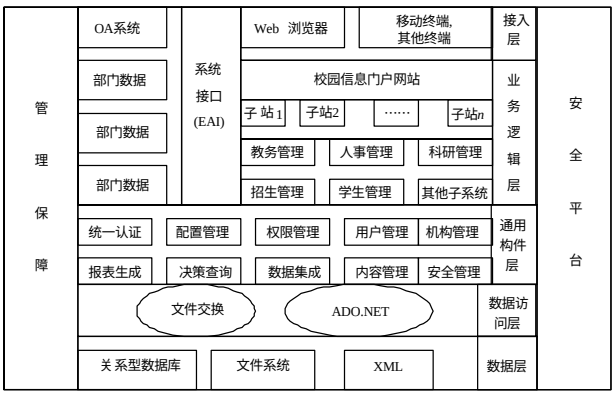

图 2　数字化校园信息门户架构

校园信息门户是对校内资源的整合，以提高资源的利用效率，也是未来校园网资源建设的一个新发展方向。信息门户涉及Portal技术、内容管理、信息检索、应用集成、单点登录和访问控制等多方面技术[1,3]。

2.2　校园 PKI/CA

安全性是数字化校园发挥应有作用的关键因素之一，非常重要。确保数字化校园的安全运行，建设一个高效、安全、可靠的校园网PKI/CA子系统至关重要；CA认证系统不仅要保证网上敏感信息传输的机密性、真实性、完整性和不可否认性，同时还要简单易用、成本低廉、性能可靠以适应数字化校园的特殊性[4~5]。

在 Linux 平台上面向校内用户开发 PKI/CA 认证系统，在校园网上实现身份认证、访问控制、机密性和不可否认等服务；以 OpenSSL 开发包作为基础密码算法的基础，在实现中采用了混合式 PKI 信任模型，着眼于 Web 方式自动管理、双重密钥对的提供、证书管理的数据库化和证书状态的实时查询等关键技术。

(1)基于 Web 的管理方式：采用 B/S 架构，客户界面和管理界面都通过 Web 界面进行。用户可以通过浏览器申请和安装数字证书，管理员可以通过 Web 界面远程管理服务器，从而实现系统的自动管理。通过浏览器实现系统的管理和服务，具有界面友好、操作方便的优点，同时极大地降低管理人员工作量，提高系统效率，增加系统的灵活性。

(2)采用双重密钥对：为每个用户产生 2 对密钥，即用于数字签名/验证的签名密钥对和用于数据加密/解密的加密密钥对。每个用户有 2 张证书，一张用于数字签名以保证信息的不可否认性；另一张用于加密，以保证信息的真实性和完整性。文章灵活处理了密钥生成，由用户生成数字签名密钥对，而由 CA 认证机构生成加密密钥对，从而既保证用户数字签名的不可否认性，又可以为用户提供加密密钥的备份与恢复功能。

(3)用数据库管理证书：传统的证书管理方案是利用操作系统本身的文件系统来实现对证书的管理。因为 X.509 证书是一个独立的语义单元，可以分别对各个证书执行管理操作，所以采用文件方式管理证书是一种很直观的方法。但是采用这种方法，系统工作效率不高，且只适用于小型系统。当用户群增大时，无论是 CA 的证书状态管理，还是证书检索，都无法保证其运行性能。采用数据库来管理证书，既简化证书管理，又提高系统的工作效率。

(4)实现证书状态实时查询：将证书状态表示成一个字段添加到数据库中，其好处是可以实现证书状态的实时查询，弥补单纯采用 CRL 方法的缺陷。

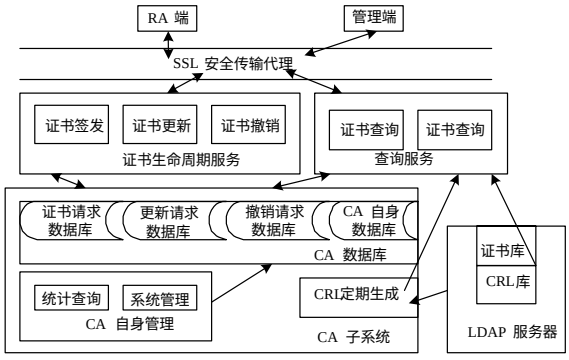

图 3　CA 系统模型及数据流程

整个认证系统的功能模块由 2 部分组成，即用户功能模块和系统功能模块。其中用户功能模块包括：用户注册，证书申请，证书查询，证书下载，证书撤消，证书验证，CRL 下载，密钥更新和密钥恢复。系统功能模块包括：CA 初始化，证书签发，CRL 发布和交叉认证。系统模型及数据流程图如图 3 所示。

2.3 数据集成

数据集成[6]的根本任务是提供用户对多种异构数据源的透明、一致和实时访问。透明性是指屏蔽底层数据源的差异，一致性是指消除数据源之间存在的结构异构和语义异构，实时性则指访问到的是最新更新的数据。数据集成是数字化校园综合应用软件平台的基础，用于集成学校各个部门支撑系统的各类数据。该解决方案是基于XML的数据集成，并且利用.NET语言实现。

XML 可以描述不规则数据，从不同的来源集成数据，将多个应用程序生成的数据纳入同一个 XML 文件并传送到客户机上，被解析出来的 XML 数据可以在本地被编辑或操纵。因此，将 XML 作为集成层的数据描述工具和转换工具来构造数据集成的中间件，不仅能够适合 Web 发展的需要，还将简化 Web 数据源集成系统的实现。图 4 所示的是一个具有普适意义的异构数据集成的体系。

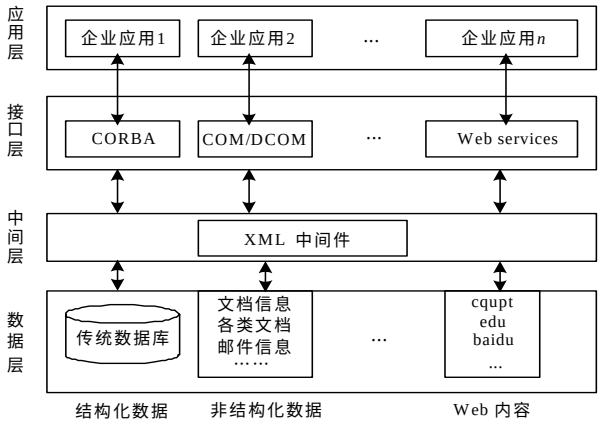

图 4　异构数据集成体系

此模型中，用户对信息的访问和操作不是直接作用各数据源，而是通过 XML 中间件(类似于虚拟数据库)来实现。通过 XML 可以集成和统一来自不同或异质数据源的信息。

如图 4 所示，系统由下至上分为 4 层结构，各层的基本服务功能如下：

(1)数据层：处于最低层，是系统的数据提供者，包括各种类型的数据库、文件、多媒体等信息。

(2)中间层：提供必要的数据转换功能或工具，进行数据与 XML 格式的相互转换，将数据存储到 XML 数据空间中，并维持 XML 数据空间与各异构数据源之间的映射关系。

(3)接口层：依据特定的协议或协作模型，负责不同应用组件请求格式的信息发布。不同的组件可以在这层被表示，不同的应用构件需要从应用级访问 XML 数据空间。一方面，实现必要的策略保持 XML 数据的一致性，从简单的读/写策略到复杂的事务操作。另一方面，接口级必须实现必要的访问控制策略以保护非法访问。

(4)应用层：即用户界面层，根据具体的应用和用户计算环境，采用合适的信息访问技术或应用软件。

由以上分析可看出，实现异构数据的集成，关键环节主要在中间层和接口层。本文选择 ADO.NET 装配件中的 DataSet 来实现这个 XML 中间件即虚拟数据库。ADO.NET 是由.NET 框架为与数据库进行交互而提供的一组对象类的名称，它可以与许多类型的对象交互，不仅可以是存储在数据库中的数据，还可以是电子邮件服务器、文本文件、程序文档(比如 Excel 电子表格)和 XML 中的数据。DataSet 是 ADO.NET 的中心概念，在内部是用 XML 来描述数据的。由于 XML 是一种平台无关、语言无关的数据描述语言，而且可以描述复杂数据关系的数据(如父子关系的数据)，因此 DataSet 实际上可以容纳具有复杂关系的数据，而且不再依赖于数据库链接。DataSet 支持多表、表间关系、数据约束等，这些和关系数据库的模型基本一致。DataSet 驻留内存中，可以将 DataSet 看做是内存中的数据库。由此可见，DataSet 具备了一个虚拟数据库的功能；由于 DataSet 基于 XML 描述，因此在系统进行异构数据集成时，在网间所需传递的数据实际上就是 XML。而 Web 服务是建立在 XML 上的，它的产生和发展有效地解决了使用诸如 CORBA 和 COM/DOOM 这样紧密捆绑的技术所遇到的问题(例如：如何通过防火墙，协议的复杂性，异构平台的集成等)，因此，系统的接口层使用 Web 服务进行数据集成。本系统的集成体系结构如图 5 所示。

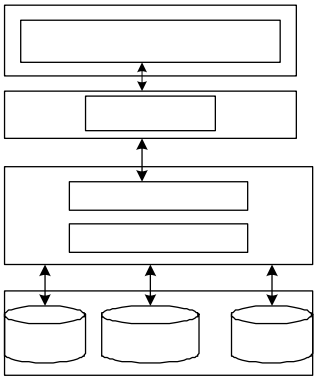

图 5　本系统异构数据集成体系结构

在接口层的 Web 服务应当具备：创建数据集(即 DataSet)；填充源异构数据到 DataSet；集成 DataSet 中的数据到目的数据源。为此，系统设计 Web 服务 IntegratedHeterogenousData 具有 CreateDataSet(), FillDataSet(), Integration()3 个方法，供客户端应用程序远程调用。考虑到该 Web 服务仅仅供本应用所使用、不必通过 UDDI 发布、不必部署到其他地方，因此将其部署在 Web 服务器上。详细的调用过程为：用户在远程客户端选择需要将异构数据集成到中央数据库某一档案类型的表，用户执行集成操作，客户端应用程序向 Web 服务器调用 CreateDataSet()，获得对应于特定类型表的 XML Schema(该 XML Schema 在该特定类型创建之初随表的创建而创建)，依据该 XML Schema 创建与此相应的 DataSet；然后应用程序调用 Fi1lDataSet()方法，将异构数据源中的数据填充到 DataSet 中；Integration()从该 DataSet 读取数据并将数据集成到中央数据库的对应表中。这样就完成了异构数据从源数据源到目的数据源的集成。

3　结束语

以本文提出的软件架构和关键技术为核心的数字化校园综合应用软件平台已经在多所大学的数字化校园建设的一期工程或二期工程中投入运行使用，实践证明该解决方案安全、可靠、运行平稳，用户满意度高。 （下转第 272 页）