第16卷 第7期
2006年7月

计算机技术与发展
COMPUTER TECHNOLOGY AND DEVELOPMENT

Vol. 16 No. 7
Jul. 2006

基于 Web Services 的证书验证系统的设计与实现

白 杨
(辽东学院 信息技术学院,辽宁 丹东 118003)

摘 要:面向用户通过 Web 验证高校证书的需求,提出了利用 Web Services 技术将当前具有不同数据结构的高校证书验证系统集成在一起的思想。通过分析查询请求的过程,将系统设计为三级结构,服务节点按三级结构进行组织。最后依据三级体系结构对系统进行了模拟实现,结果证明证书验证系统设计是可行的,并且拓展了 Web Services 技术的应用领域。

关键词:Web services;XML;SOAP;WSDL;J2EE
中图分类号:TP393.09 **文献标识码**:A **文章编号**:1673-629X(2006)07-0138-02

Design and Realization for Certificate Validation System Based on Web Services

BAI Yang
(College of Information Technology, Liaodong Institute, Dandong 118003, China)

Abstract: For user's demand to validate certificate about educational level and degree through Web, the notion to integrate current certificate validation systems about educational level and degree with different data structure via Web services is proposed. The system structure of three level is designed based on the analysis of search require process, and service node is organized according to the system structure of three level. Finally the prototype system is built and experimented to prove that the design of certificate validation systems is feasible. The application field of Web services technology is enlarged by this research.

Key words: Web services;XML;SOAP;WSDL;J2EE

0 前 言

随着国内假学历学位证书的大量出现,国内的教育管理部门和高校建立了学历学位证书网上验证系统。现有的证书验证系统有两种方式:一种方式为证书信息存放在高校,此系统只能验证此高校颁发的证书;另一种方式为通过电子注册方式把多个高校的证书信息存放到集中数据库中,可以验证多个高校颁发的证书。以上两种方式都有很大的不足,用户使用很不方便。第一种方式在对不同高校颁发的证书进行验证时,需要登入不同的 Web 站点,很烦琐。第二种方式维护数据不方便,并且存在单点故障的问题,由于以前证书的编号没有规范,此方式只能验证规范证书编号的证书。那么如何将 Web 上处于不同系统平台上的证书验证系统互连集成在一起,使用户通过任何一个系统都可以验证任何高校颁发的证书,已成为当务之急。文中利用 Web Services 技术和 J2EE 架构解决了这个难题,提出了构建基于 Web Services 的学历学位证书验证系统的模型框架,并对此模型框架进行了设计和实现,结果证明提出的模型框架是可行的。

收稿日期:2006-01-11
基金项目:辽宁省教育厅基金资助项目(2004D115)
作者简介:白 杨(1973-),女,辽宁丹东人,讲师,硕士,从事计算机数据库及网络研究。

1 Web Services 技术

针对现有证书验证系统的不足,文中提出采用当前新的分布计算和应用技术 Web Services 将现有的 Web 上的各高校的证书验证系统和即将建立的证书验证系统集成在一起,充分利用 Web Services 技术的跨平台和通过 HTTP 和 SOAP 实现 RPC 的特性,在各系统的应用程序之上加一 Web Services 实现的表示层,将各系统的应用程序互连起来。下面概述 Web Services 技术。

根据 W3C 的定义,Web Services[1] 是可以通过一个 URI 识别的软件系统。它的公共接口和绑定由 XML 定义和描述。它的定义可被其它软件系统所发现。这些系统可以与其它的系统以一种由它的定义所指定的方式通过基于 XML 的由 Internet 协议所传输的消息而相互作用。作为基于 XML 的实现分布计算技术[2] 的 Web Services,主要思想是利用开放的、标准的 Web 规范与协议(包括 HTTP,XML,SOAP,WSDL 和 UDDI 等),实现将处于不同的物理地点、不同的物理设备和不同的操作系统及开发平台上用不同的语言和工具开发的应用程序在 Web 的松散耦合环境中实现分布式计算和集成。文中利用此技术实现将现有的学历学位证书验证系统互连和集成在一起。

2　系统的设计

2.1　节点定义

文中按照业务隶属关系将现有和即将构建的各系统称之为一个节点,将节点分为如下三级:一级为教育部节点;二级为省(直辖市)节点;三级为高校节点。其中二级节点有多个,三级节点有多个。为了使生成的总服务代理类的数目较少,系统部署较容易,定义节点间的通信规则:

(1)一级节点只与二级节点直接通信。

(2)二级节点可与一级或所管的三级节点直接通信。

(3)三级节点只与所属的二级节点直接通信。

并假设其中每个节点中存放证书信息的数据库和对证书信息进行查询的 Web 应用程序。

2.2　查询请求的过程分析

可以对查询请求的处理过程总结为两种策略:请求/响应,分发/提交。查询请求的入口点分别为以上的三级节点,由于证书编号是证书信息的唯一键值,通过编号能够确定证书所属的省份和学校。当用户提出查询请求时,三级节点处理查询请求的过程是:

(1)当一级节点接收到入口查询请求时,查询本地数据库,如查询到则返回证书的信息给请求者;如查询不到,一级节点可以根据证书编号判断将查询请求发给某一二级节点,然后接收响应。

(2)当二级节点接收到入口查询请求时,查询本地数据库,如查询到则返回证书的信息给请求者;如查询不到根据证书编号判断是否是所管理的某一三级节点,如是将查询请求发给此节点;如判断不是将查询请求提交给一级节点,然后接收响应。

(3)当三级节点接收到入口查询请求时,查询本地数据库,如查询到则返回证书的信息给请求者;如查询不到将请求提交给所属的二级节点,然后接收响应。

每级节点的分发/提交过程不同。由于 Web Services 的 SOAP 消息基于请求/响应模式,并且能够实现对 Web 上远程应用程序的 RPC 调用,在这里可以理解为调用其他节点处理查询请求的应用程序,因此可以利用 Web Services 实现将以上三级节点互连。实现步骤如下:用 SOAP 请求消息表示查询请求中的查询实参,把对相应节点的分发和提交表示为 RPC 调用,用 SOAP 响应消息表示查询响应的证书信息的结果集。实现 SOAP 消息需要 Web Services 的支持,因此这里把处理查询请求的模块表示为 Web Services,即此模块可以被其他远程模块通过 HTTP 和 SOAP 消息而调用。这里把每一节点的处理查询请求的模块定义为一个 Web Services。

2.3　节点的层次结构

由于 Web Services 基于服务请求者、服务提供者和服务中介者三个角色的模型,文中将服务请求者的角色划分为如下三类:服务、Web 应用程序和桌面应用程序。对用户而言,可以使用浏览器通过 Web 应用程序或桌面应用程序(绑定了 HTTP 功能),使用 Web Services 的功能。而各服务之间是对等关系,并将各节点互连起来。文中将每个节点划分为三层结构,分别为表示层、操作层和数据层(如图 1 所示),其中操作层负责查询数据库;表示层中的 Web Services[3] 负责查询请求的分发、提交和将参数传递给操作层,Web 应用程序接收查询请求,调用 Web Services,最后把结果通过 HTTP 返回给用户。Web Services 和 Web 应用程序都部署在 Web 服务器中,以充分利用 Web 服务器接收 HTTP 请求和响应。

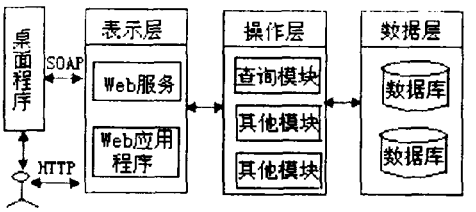


图 1　节点的三层结构

3　系统的实现

系统中每层节点的数据库都可能存放证书信息,但一级节点还需存放二级节点的省份编号,二级节点还需存放所包含的三级节点的编号。高校信息表、省级信息表及学生证书表构成了数据层。而操作层的实现用 J2EE 中的 EJB[4,5] 来实现 validation 查询方法,主要代码如下:

(用 Java 定义相应的两个类 Certificate 和 Certi_info 的代码略,以上两类分别代表需验证的证书信息和返回的证书信息。)

```
Public Certi_info validation {
  Throws finderException{
  Connection con=null;
  Try{Con=getConnection();/*连接数据库*/
PreparedStatement statement = con. PrepareStatement ("SELECT * " + "FROM Certificate_info WHERE num=" + certi. num+"and name=" + certi. name+"and sex=" + certi. sex+"and birth_time=" + certi. birth+"and entry_time =" + certi. entry + "and gradute_time=" + certi. gradute_time+"and school=" + certi. school+"and major=" + certi. major);
  ResultSet resultSet=Statement. executeQuery();
    While (resultSet. next()){
    Certi_infocerti_info = new Certi_info(resultSet. getString (1),...){
    ResultSet. close();
    Statement. close();
    Return certi_info;/*返回结果*/
      }catch (SQLException sqle){
    throw new EJBException(sqle);}
  ……}
```

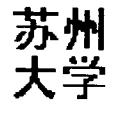
表示层的实现包括三级节点中每级表示层的实现,其中每层服务的设计包括如下几个步骤:

(1)通过远程服务的 WSDL 文档生成被调用服务的代理类 stubs。

(2)在服务中创建 stubs 类的对象。

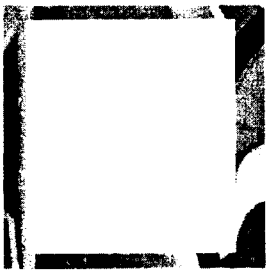
(下转第 143 页)

(a) 未受攻击的嵌入水印后图像



(b) 提取出的水印

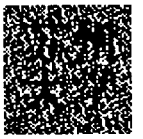
图 4　未受攻击的实验图像



(a)遭受大面积的剪切攻击的嵌入水印的图像

(b) T=0.01

(c) T=0.13



(d) T=0.5

图 5　遭受攻击后的提取图像

正确提取时,嵌入"1"提取出"1",或者嵌入"0"提取出"0"。错误提取时,嵌入"1"提取出"0",或者嵌入"0"提取出"1"。随着图像被破坏程度的加剧以及破坏范围的增大,正确提取的概率变小,而错误提取的概率变大。水印图像嵌入过程中排列了 max 次,在每一次排列中,由于遭受攻击,提取出的图像可能无法辨认,而在相应位置的其他的排列中,却很有可能是正确的。max 次排列的图像,对于水印图像上每个像素点,有 x 次正确提取,有 y 次错误提取,$x + y = \max$。可见水印信息排列的次数 max 对于检测的成功率非常重要。嵌入水印图像排列的次数越多,就越能够拉开错误提取次数与正确提取次数的差距,也就越能够抵抗对水印的攻击。在遭受攻击后,应该选择一个中间值进行分割,一定存在一个阈值,使得提取出的图像与原水印图像最接近。

3　结束语

实验表明,文中提出的基于小波变换的图像鲁棒性盲水印算法,能够很好地抵抗对图像局部剪切的攻击。当图像的一部分遭到攻击之后,其他未遭受攻击的部分的嵌入信息仍然能够正确地提取。只有当所嵌入区域的信息全部被破坏时,水印才无法提取,鲁棒性也就失去。实验表明在(0,1)之间存在一个值 X,使得当 $T = X$ 时,提取的水印图像具有最好的质量。

参考文献:

[1] Cox I J. 数字水印[M].北京:电子工业出版社,2003.

[2] 常　敏. 数字图像水印综述[J].计算机应用研究,2003(10):1-3.

[3] 侯振华,陈生潭.脆弱性数字水印研究[J].计算机应用,2003,23(12):106-108.

[4] 刘瑞祯,王蕴红,谭铁牛.基于图象内容的数字水印模型[J].中国图象图形学报,2001,6(6):556-562.

[5] 李　兵,徐家伟.Arnold 变换的周期及其应用[J].中山大学学报(自然科学版),2004,43(2):139-142.

[6] 刘振华,尹　萍.信息隐藏技术及其应用[M].北京:科学出版社,2002.

[7] 纪　震,李慧慧,肖薇薇,等.基于混沌序列的数字水印信号研究[J].电子学报,2004,32(7):1131-1134.

[8] 张家树,田　蕾.一种新的基于密钥的混沌数字水印方法[J].通信学报,2004,25(8):98-101.

[9] Wolfgang R B,Podlchuk C I,Delp E J. Perceptual Watermarks for Digital Images and Video[J]. Proceedings of the IEEE. 1999,87(7):1108-1126.

(上接第 139 页)

(3)根据接收的查询请求初始化 EJB 组件或对查询请求分发,对查询请求分发的处理就是调用相应 stubs 对象的 certi_wm 方法,传递的参数就是接收的查询请求。

(4)最后将 stubs 对象的非空返回结果给调用者,如果有多个不为空,合并结果集或构造错误消息给调用者。

4　结束语

利用 Web Services 技术将 Web 上现有的学历学位证书验证系统集成,设计并实现了证书验证系统,方便用户的查询。系统的实现对基于 Web Services 的技术应用研究有一定的借鉴意义。

参考文献:

[1] 郑小平..NET 精髓-Web Services 原理与开发[M].北京:人民邮电出版社,2002.

[2] 陈锦辉,王景皓.XML 与 JAVA 程序设计大全[M].北京:中国铁道出版社,2002.

[3] 郑晓东,王志坚.一种基于 Web Service 的分布式计算模型研究及其实现[J].计算机工程与应用,2004(1):144-147.

[4] Allamaraju S. J2EE 服务器端高级编程[M].闻道工作室译.北京:机械工业出版社,2001.

[5] Girdley M. J2EE 应用与 BEA WebLogic Server[M].邢国庆等译.北京:电子工业出版社,2002.