

电子政务分布式应用集成框架研究^{*}

毛 庆 冯德民 王映辉

(陕西师范大学计算机学院 西安710062)

摘 要 随着计算机技术和网络技术的发展,电子政务的开发模式发生了很大的变化。分析了目前已有的基于网络计算模式在构架电子政务中存在的不足和缺陷;针对电子政务分布式数据和应用集成的需求,分别给出了基于消息交换中心的应用集成方案和基于区域代理服务器的数据集成方案,阐述了它们的组成机理,为电子政务应用的分布式集成提供了一种通用的集成策略。

关键词 电子政务,多层结构,Web 服务,消息,集成

Study on Distribution Application in Tegration Framework of the Electronic Government

MAO Qing FENG De-Ming WANG Ying-Hui

(Department of Computer Science, Shanxi Normal University, Xi'an 710062)

Abstract Many changes of E-government development model have happened as computer&network technology developing. Analyze limitation of present network computing model using in E-government. Under requirement-driven of E-government distribution application&data, an integration strategy is drawn based on message exchange center and a agent server of region, describing mechanism of this integration strategy. This integration strategy is still common strategy for other districbution application.

Keywords E-government, Multi-tier architecture, Web Services, Message, Integration

1 引言

随着计算机技术和网络技术的发展,电子政务技术蓬勃发展,并被日益运用到政府各种行为中。政府通过电子政务的实现,不断提高工作效率,同时,人们也从中享受着由此带来的方便。特别是近几年,我国已将建设电子政务作为社会经济信息化的突破口^[1],政府在逐步利用电子网络实现政府意志。然而,由于政府机构行政体系的划分,以及政府地域的不同和差异,各地政府都在致力发展本地的电子政务,缺乏统一的协调和规划,使得电子政务系统的大量数据资源分散在各个职能部门,形成了一个又一个的“信息孤岛”,无法在电子政务网上有效地共享^[1,2]。信息孤岛的存在,导致了信息化建设的重复投资,并进一步产生了不同部门中同一个用户数据的不一致性等问题;加之电子政务发展的长期性过程,致使目前电子政务的发展和实施过程面临着一系列严峻的问题,特别是如何有效地利用已有的资源(数据资源和软件资源)是目前最令人关注的,也是电子政务目前棘手需要解决的问题,其实质是对已有资源的集成问题。

本文首先分析了近几年来电子政务的几种发展模式,并指出它们在解决电子政务信息孤岛问题时存在的缺陷。进而根据当今计算机分布式技术的发展,结合目前电子政务的实际需求,给出了电子政务分布式应用集成框架方案,并对其集成机理进行了详尽的描述。

2 电子政务模式的演变

我国传统的政府工作模式是基于纸质传递的办公模式,

由于科学技术的发展,同时由于社会进一步发展的需要,政府上网、政府电子办公也迅速发展。电子政务正是在这种社会大环境下发展起来的,政府作为国家的权力中心和社会管理机构,正在从管理型到管理服务型转变。政府机构除了管理和规范国家政治经济活动之外,将借助强大的网络技术,把更多的时间和精力,投入到社会公众服务中去。社会信息资源和各种政策法规不再会在“尘封库”中或者是层层传达,而将通过网络在第一时间与公众见面,通过网络,政府可以广纳贤言,迅速了解社会政治经济的发展动态,甚至是来自社会最底层的信息,并以此做出及时准确的决策,这将更好地促进经济建设和社会稳定。

因此,电子政务是基于 Internet/Intranet 技术的综合信息系统^[3]。它一方面要面向政府部门,处理它们的各种业务请求;另一方面,它还要面向社会公众和企业的,为社会公众和企业提供相应的服务,处理社会公众和企业所提出的各种请求。图1是电子政务的基本模型。

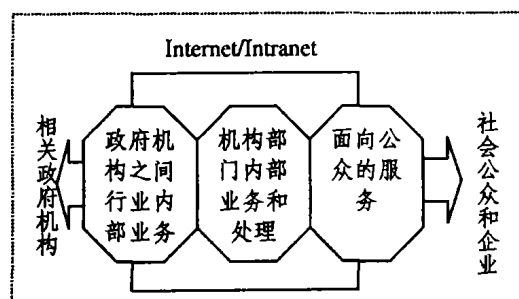


图1 电子政务基本模型

^{*} 本文获陕西省自然科学基金(2003F35)和国家 863 重大专项基金(2003AA118105)资助。毛 庆 硕士研究生,主要研究方向为分布式集成技术。冯德民 教授,主要研究方向为分布式集成技术与计算理论。王映辉 副教授,主要研究方向为软件工程、软件演化与 WebGIS 技术。

从图1中可知,首先,电子政务必须面向社会公众和企业,这是电子政务的基本目标;其次是充分利用机构内部的办公自动化及业务信息系统,更快更好地为市民及企业服务,提高工作效率。此外是利用 Intranet 和 Intranet 将政府机构连接在一起,协同工作,达到高效的、高质量地为社会公众和企业服务。

从图1中还可以发现,电子政务系统是由许多基本服务单元的集成,这样的基本服务单元(也叫电子政务服务节点)就是一个基本的政务服务程序或者是一个业务的基本服务系统。但是电子政务节点的概念和传统的信息系统有所不同,它不仅为本地的用户完成应用的业务处理,同时还可以被其它本地或异地的系统应用所调用。

在电子政务的发展过程中,电子政务基本服务节点大致经历了以下几个阶段: C/S 模式阶段、B/S 多层结构模式阶段和 Web Services 模式阶段。

2.1 C/S 模式

传统的政府信息应用是客户服务器模式,它主要是由数据库服务器和传统客户终端构成的两层结构模式。数据库服务器主要处理用户对它的各操作以及对它自身的维护,传统的客户端不仅包括用户界面,还包括具有应用的业务逻辑。

但这种系统结构相对简单,开发成本也较低,在业务量较小的部门有较多的应用。但是随着业务量的发展,客户终端的增加,或者应用系统的升级,系统就会出现性能降低、维护成本增加、系统可靠性减弱并出现极大的不稳定性;另外,在这种结构中几乎所有的应用逻辑都在客户端实现^[4],导致客户端应用程序越来越复杂,维护这样的工作是一项庞大的工作。

2.2 B/S 多层结构模式

B/S 多层结构的应用系统是在客户服务器模式的基础上将传统客户终端中的业务逻辑和用户界面独立出来,形成了以业务逻辑为核心的应用服务器,而终端成为了操作界面的瘦客户终端,可以是 Java 终端,也可以是由 VB、Delphi 等编程的客户终端。如果在这个系统中增加了 Web 服务器,用 HTML 或 JSP 等作为描述性编程语言,连接 Internet,用户端就可以是浏览器通过互联网操作应用系统^[4]。

B/S 多层结构与传统 C/S 结构相比有许多优势^[5~8]。首先实现了瘦客户端,它无需像 C/S 模式那样在不同的客户机上安装不同的客户应用程序,而只需安装通用的浏览器软件即可;同时简化了系统的开发和维护,各个用户通过 HTTP 请求在权限范围内调用 Web 服务器上不同处理程序,从而完成对数据的查询或修改。相对于 C/S,多层体系结构具有更大的灵活性和适应性。

但是这样的系统还是不能成为基本服务节点,因为用户只能通过应用客户端(不管是浏览器还是其它客户端程序)操作应用系统,其服务还是无法被其它应用调用。一般说来,一个服务要被其它应用调用,必须向其它应用公布它的计算环境、数据结构、调用规则等相关参数,由于计算机技术的发展受到社会潜在规则的影响,几乎所有计算机产品或多或少都有兼容性的问题,因此不同应用系统的相互调用至今仍未彻底解决。

2.3 Web Services 模式

只有当 Web Services 技术和 XML 语言的出现使得应用之间的相互调用成为可能。

Web Services 是建立互操作分布式应用程序的新平台。利用这样一个平台,不管客户端与服务器处于怎样的环境,都

可以通过用 HTTP 协议来解决客户端与服务器之间的通信问题;另一个方面,还可以解决应用程序间的互操作问题。

可扩展的标记语言(XML)是 Web Service 平台中表示数据的基本格式,XML 将数据转换成通用格式,方便不同系统之间的信息交流。XML 除了易于建立和易于分析外,其主要的优点在于它既是平台无关的,又是厂商无关的。

简单对象访问协议 SOAP(Simple Object Access Protocol),提供了标准的 RPC 方法来调用 Web Services。简单地说,SOAP 是一种有线协议,类似于 CORBA 的 IIOP、DCOM 的 ORPC 或 Java 的远程方法协议 JRMP(Java Remote Method Protocol)。

以上各种技术和协议的出现,为电子政务应用集成奠定了基础。

3 电子政务分布式应用集成策略

解决信息孤岛问题的最直接的办法是彻底推翻现有的应用体系,重新建立一个统一的、大而全的应用系统,这对于绝大部分的企业或政府是不现实的。为了能够共享其它应用系统的数据,一般的方法是直接打开目标应用数据库读写数据。如果在企业或政府应用系统较多而且复杂的情况下,就会形成复杂的点对点的网状拓扑结构。这种一对一的直接读写或调用的方法,使得一个系统对另一个系统的依赖,系统之间的相关性很高,进而使系统维护复杂,一旦一个系统的结构发生了变化,就会导致另一个系统的异常。另外,由于应用系统为了共享而开发数据环境,有可能存在数据被恶意破坏的隐患。

因此,如何让应用系统之间很好地共享数据,这是企业分布式应用集成的一个关键,其核心是数据集成和应用集成,下面给出这两种集成的具体方案。

3.1 应用集成模型及其运行机理

在典型的 Web Services 结构中,当 SOAP 客户端(存在于任何一个应用系统内)通过任意的传输协议将 XML 格式的请求文档送到 SOAP 服务器,当 SOAP 服务器收到请求文档,并解析这个文档所描述的请求,并调用应用服务器中的应用代码,读写操作内容或数据,并将应用的响应文件送回 SOAP 客户端。而 SOAP 客户端并不关心应用服务器是什么应用环境,什么语言开发,什么体系结构等。

由此可见,只有在应用服务器增加一个 SOAP 服务器,可以将原来的节点变成一个基本的服务节点。另外,再增加一个总的消息交换中心,各基本服务节点通过消息交换中心相连,进而形成一种星型结构(图2)。

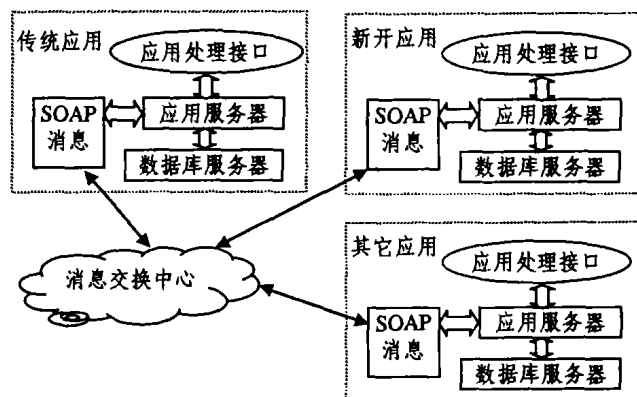


图2 基于消息交换中心的分布式应用集成模型

图2是一个利用消息交换中心为基础的分布式系统集成

方案。在这个图中采用了典型的星型结构,中心结点为消息交换中心,它为各应用程序提供一个通用的数据交换接口。应用程序除了调用自身的资源外,还可调用其它应用程序,为此,应用程序首先将自己的请求根据相应协议转换成基本格式的消息,传递给消息交换中心,消息交换中心对传递来的消息进行相应的解析,分析相应的请求,并传递给相应的服务系统,服务系统调用应用服务器中的应用代码,读写操作内容或数据,并将应用的响应文件再通过信息交换中心返回调用的应用程序。

从图2可以看出,由于缺乏规划而造成的混乱的数据流不见了,代之以消息传输及应用信息交换中心。所有的应用都和交换中心相连,任何一个应用数据请求通过这个交换中心传递到相应的目的应用,任何一个消息可以在交换中心按照要求转换成所需的数据结构,再传输给目的应用系统。

当然,以消息交换中心为核心点的交换体系,存在单点故障问题。在实际设计中,可通过“辅助信息交换中心”来解决单点故障问题。辅助信息交换中心起到冗余备份作用,一旦消息交换中心的核心机器或系统出现故障时,马上接管核心机器的任务,为其它程序提供交换等服务。

3.2 数据集成模型及其运行机理

在电子政务平台实施中,考虑到数据分布在不同的部门及应用系统中,为了有效地管理和利用数据,在数据服务器之间设置了一个区域代理服务器,进而形成的体系结构如图3所示。

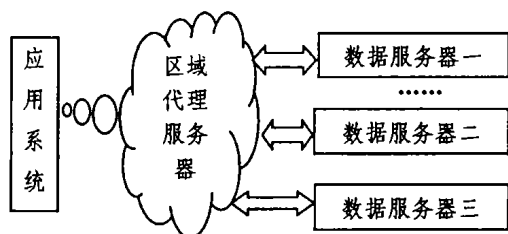


图3 分布式数据集成模型

图3是分布式环境下数据集成的模型。区域代理服务器通过消息的传送到与数据服务器和客户应用之间的数据交换。通过区域代理服务器使得各数据服务器形成一个整体,从而实现各应用系统间的数据有效交互与共享。当集成环境中某个应用程序对数据对象进行了更新、删除等更改操作时,最新的数据应该发布到其它对该数据对象感兴趣的应用程序。而当一个应用程序需要从其它应用系统主动获得数据或是进行数据查询时,该应用程序将首先发出对这些数据对象的请求,然后等待数据对象提供者做出应答。这些活动都是通过区域代理服务器来完成的。

利用图3可以实现数据的集成。首先解决数据孤岛的问题,使分散的数据以区域代理服务器为桥梁,通过数据服务器的协调工作成为一个整体;其次解决了数据的不一致问题,在图3中通过区域代理服务器可以使数据一旦发生变化,其它数据服务器都可以得到相应的更新;另外利用数据集成还可以解决其它一些问题,像数据的收集与报送的高成本和低效率的过程以及不能连接的应用将增加维护成本等问题。

当然,以区域代理服务器为核心点的交换体系,同样存在单点故障问题,在实际设计中,其采用类似于应用集成中单点故障的解决方案。

3.3 集成的整体模型

通过信息交换中心和区域代理服务器,可以非常方面地完成电子政务中应用软件系统和数据的集成问题。其整体集成模型如图4所示。

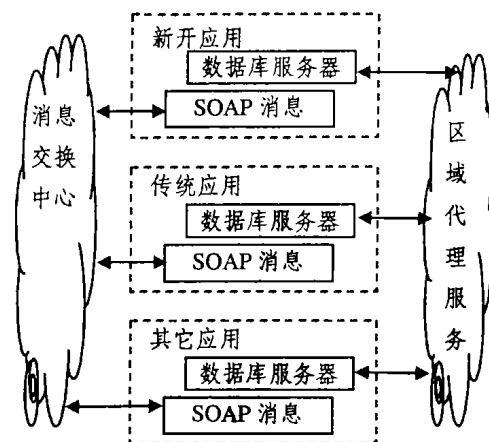


图4 整体集成模型

图4给出了在分布式环境下,特别是在 Internet/Intranet 环境下电子政务中集成的一个整体模型,它实质上是一个有效的协同集成环境。

不同应用系统完全可以通过信息交换中心,利用 XML、SOAP 等协议和技术完成松散式的协同工作;而各种数据库服务的整合、应用与一致性问题的解决是通过区域代理服务器来完成的。

3.4 集成策略的优点

利用消息交换中心和区域代理服务器机制,构建电子政务分布式整合集成平台,其优点是:①通过信息交换中心,完成了不同应用系统(新的和老的)的协同工作;通过区域代理服务器,完成了各种数据库服务的整合和应用;②为电子政务的大规模应用构架提供了数据和应用的具体集成方案;③任何系统将不对其它应用开放,避免可能的恶意修改和破坏;④一个应用系统的修改或升级,将不影响其它应用的继续运行;如果发生数据结构的变化,可应用交换机制将数据结构转换成新的格式而不需要修改应用,减少维护成本;⑤由于系统结构的清晰,简化了编程、排错与纠错工作量,降低了应用开发与整合的成本;⑥增加了系统扩展的能力。由于新的系统与旧的系统没有必要从系统结构、系统环境方面发生关联,因此,将有利于应用系统的无限制扩张。

结束语 分布式应用集成和数据集成问题是当前分布式应用软件要解决的重点和难点问题。一方面人们不断地开发着新的应用软件,另一方面摆在人们面前的任务是对已有软件的利用,这就需要我们提供一种集成策略,能够将目前所产生的和已有的应用软件加以融合和集成,使得应用软件能够相互调用,资源得到合理利用。本文正是从目前电子政务集成需求出发,针对“信息孤岛”问题,结合实际应用,给出了分布式应用集成的具体解决方案。

集成技术是大规模软件构架的核心内容^[6]。现今电子政务正处于蓬勃发展之中,也属于大规模软件构架的范畴。电子政务随着技术发展与人民生活越来越贴切,如何建立一个符合各方面需求的分布式电子政务平台是目前我国政府部门所关心的核心问题,文中的集成策略是一种有效的解决途径。

另外要说明的是,虽然该集成策略产生于电子政务建设的需求中,但它具有一定的通用性,对其它各种分布式应用系统的集成有同样重要的参考价值。该集成方案已在西安市某

县的电子政务构架中得到了验证和应用,并取得了良好的效果。

参考文献

- 1 张清浦.西部大开发与政府 GIS[J].测绘科学,2000,25(2):37~42
- 2 陈拂晓.电子政务与标准化—我国电子政务建设面临的机遇与挑战.信息技术与应,2003,(1-2):14~17
- 3 张震.网格技术及其在电子政务平台中的应用[J].电子技术,

(上接第87页)

$(K_{CV}, N', W_o, Expiry)_{K_{CB}}$

经纪人将 N' , W_o , $Expiry$ 和 W_N 存储在数据库中,并从用户 C 账户上扣除与散列链数额相当的资金,并将其转移到用户 U 的账户上。同时,经纪人发送如下支付授权消息给商家。

$(ID_C, ID_B, N', W_o, K_{CV}, Expiry, OI)_{K_{VB}}$

商家验证授权消息的合法性,并保存 N' , W_o , W_N , $Expiry$, OI 和 ID_C 。支付与存款过程可参照前节有关协议。

PayWord 方案中没有提及可转移性,消费者生成的 PayWord 链通常都是针对特定商家的,且不能将其转让给其他用户。

4.2 公平性

本文所提出的系统预付系统,它假定经纪人是诚信的,消费者在获得商品或服务之前将相应的资金支付给经纪人,因而商家和经纪人的利益得到了很好的保障。交易所散列链是由经纪人产生的,消费者的超支消费问题也得到解决。同时,由于在和消费者进行交易前商家需要经纪人的授权信息,并能够通过遍历数据库验证消费者支付指令的合法性,在支付结束时删除对应于该消费者的经纪人授权信息,从而有效地防止了消费者进行重复花费。综上所述,本文所提出的系统对于客户和商家都是公平的。

而 PayWord 方案并没有为参与交易的各方提供真正的公正性。在 PayWord 方案中,由于它是基于信用的,消费者在付款之前已获取了商家所提供的信息商品或服务,因而存在着消费者的重复花费和超支消费等欺诈行为,对于经纪人和商家都是不公平的。

4.3 安全性

由于每次支付执行时,交易信息都是使用共享密钥进行加密的,因此攻击者无法获取相关的敏感信息,也无法伪造合法的电子现金。同时,商家无法进行重复存储,由于存款协议执行结束时,经纪人已将数据库中用户条目中的 W_o , OI , $Expiry$ 和 W_N 删除且商家不知道 C 和 B 共享的秘密密钥 K_{CB} ,因而无法通过经纪人的合法性检验。由前面的分析可知,本系统同样能够防止用户进行重复花费和超支消费。

PayWord 系统中支付承诺是使用用户的私钥进行签名的,且由于散列函数具有单向不可逆性,因而能够有效防止攻击者的伪造和非法花费。经纪人通过数据库的形式存储某一支付承诺及其对应的已花费的 PayWord,能够有效地防止用户重复花费和商家的重复存储。

4.4 效率分析

在本系统中,用户不需要经纪人签名的证书,而仅仅需要与经纪人共享一个秘密密钥 K_{CB} ,用户的支付承诺(用户对支付指令的签名)转换为用户使用对称密钥对支付指令进行加

2003,7:22~23

- 4 王卫军,付晓江.基于三层体系结构电子政务系统的 JSP 技术[J].吉林大学学报(信息科学版),2003,21(1):87~91
- 5 曾喻江,谢自美,盛翔智.电子商务网站中的三层体系结构[J].信息技术,2001,11:32~34
- 6 王映辉,冯德明.大规模软件构架技术[M].科学出版社,2003
- 7 王映辉.分布构件模型技术比较研究[J].计算机应用研究,2003(7)
- 8 王映辉.基于 Web 的应用程序构造模式比较研究[J].计算机科学,2003(7)

密。在协议执行过程中,散列运算的次数基本上与 PayWord 相同,且商家和经纪人保存的信息也很简单,并在协议执行完成后即可进行删除,因而计算开销和存储开销大大减少。在 PayWord 方案中,每个用户需要一个由经纪人签名的数字证书,且在每次支付时,都需要用户签名生成一个支付承诺,用户、经纪人和商家都需要进行 N 次散列运算。为防止用户进行重复花费,经纪人和商家需要记录和保存最后一次消费的有效 PayWord、支付承诺及数字证书等信息,计算开销和存储开销较大。所以,本文所提出的微支付系统,由于完全没有采用公钥密码算法,其效率大大提高。

4.5 有限的匿名性

由于只有经纪人知道用户的匿名标识和真实身份之间的对应关系,因而在与商家进行交易时,商家不能获知用户的身份信息,所以系统为用户提供了有限的匿名性。在 PayWord 方案中,由于经纪人颁发给用户的数字证书中包含了用户的身份信息,因而系统没有提供匿名性服务。

结论 本文设计了一个基于散列链的高效微支付系统。该系统是一个离线的预付系统,它采用秘密密钥加密体制及相关的技术手段来防止用户的重复花费、超支消费和商家的重复存储,为参与交易的各方提供了安全保障。与现有的微支付方案相比,由于它完全没有采用公钥密码算法,且协议执行中所需保存的信息比较简单,因而系统的计算开销和存储开销大大减少。此外,由于系统允许用户在开户时使用匿名标识,该标识与用户的真实身份没有必然联系,在进行交易时,商家无法获知用户的身份信息,因而系统提供了有限的匿名性。

参考文献

- 1 Herzberg A, Yochai H. Mini-Pay: charging per click on the Web. In: Proc. of the 6th Intl. World Wide Web Conf. Santa Clara, California, April 1997. 301~307
- 2 Azbel. PayWord micro-payment scheme: strengths, weaknesses and proposed improvements. Department of Computer Science, University of Cape Town, South Africa, 1997
- 3 Burstein J. An implementation of MicroMint: [M. Sc thesis]. Massachusetts Institute of Technology, Cambridge, Massachusetts, May 1998
- 4 Buttyán L. Removing the Financial Incentive to Cheat in Micro-payment Schemes. IEE Electronics Letters, 2000, 36(2): 132~133
- 5 Manasse M. The Millicent protocols for Electronic Commerce. In: Proc. 1st USENIX Workshop on Electronic Commerce, New York, 1995. 117~123
- 6 Adachi N, Aoki S, Komano Y, et al. The Security Problems of Rivest and Shamir's PayWord Scheme. In: Proc. of the IEEE Intl. Conf. on E-Commerce (CEC'03), 2003. 126~129
- 7 Rivest R L, Shamir A. PayWord and MicroMint: two simple micropayment schemes. Lecture Notes Comput. Sci., 1997, 1189: 69~87
- 8 Glassmann S, Manasse M, Abadi M, et al. The Millicent protocol for inexpensive electronic commerce. In: Proc. of the 4th Intl. World Wide Web Conf. Boston, MA, 1995. 603~608
- 9 Yen S, Lee C, Ho L. PayFair: a prepaid Internet micropayment scheme promising customer fairness. In: IEE Proc. of Comput. Digit. Tech., 2001, 148(6): 207~213