数据交换与安全身份认证在护照签证管理系统中的应用研究

宋兆辉[1] 吴剑栋[2] 郑 宁[1]
[1](杭州电子科技大学计算机学院 浙江 杭州 310012)
[2](上海信息投资咨询有限公司 上海 200002)

摘 要 分析当前电子政务网上办事系统的发展现状及特点,结合护照签证管理信息系统的使用现状与发展要求,确定了基于网闸数据交换的系统架构。全面研究系统的结构与功能,并采用基于智能 key的多项安全技术,保证了系统的易用性,可靠性、安全性与扩展性。

关键词 电子政务 数据交换 身份认证 护照 签证 系统研究

RESEARCH ON DATA EXCHANGE AND REMOTE IDENTIFICATION BY INTELLIGENT KEY IN PASSPORT AND VISA MANAGEMENT INFORMATION SYSTEM

Song Zhaohui[1] Wu Jiandong[2] Zheng Ning[1]
[1] (College of Computer Science, Hangzhou Dianzi University, Hangzhou 310012, Zhejiang, China)
[2] (Shanghai IT Investment Consulting Co., Ltd, Shanghai 200002, China)

Abstract The characteristics and the status quo of e-government systems are analyzed. Referring to the passport and visa management information system, an architecture of data exchange based on GAP is presened. Intelligent key is applied to realize remote identification. These security technologies have improved the convenience, reliability, safety and extensibility of the system.

Keywords E-government Data exchange Identification Passport Visa System research

0 引 言

随着电子政务的进一步发展,政府的网上办事已经不仅仅局限于网上简单信息查询、相关表格下载等,而是逐步走向"外网受理,内网办理,外网反馈"的模式。由于外网(互联网)与政府内网的涉密域不同,一方面是为了实现实时性,要求外网填报的数据能及时地传送到内网进行处理,并把处理结果及时地反馈到外网;另一方面是政府内部网络对数据的安全性和保密性有着严格的要求,并且严格规定互联网与政府内网之间要实现物理隔离。因此,如何能在保证安全的前提下,做到内外网之间的数据交换就成为当前电子政务中比较重要的一个问题。此外,如何实现对远端授权用户的身份进行验证,减少垃圾数据的产生,保证系统的正常运转也是在网上办事系统中应该重点关注的一个问题。

本文通过对护照签证管理信息系统的剖析,介绍了在不同涉密域的情况下,如何实现内外网之间的数据交换及基于智能 key的远端身份认证。

1 系统分析

1.1 用 户

因公出国护照签证管理信息系统的用户可以分为两类:一是受理护照签证事务的工作人员(以下简称受理人);二是全市有因公出国派出权的各申报单位的申报专管员(以下简称专管员)。

1.2 现状及需求

经过调研,得知原有的申报过程是各单位的专管员携纸质申报材料到申报大厅办理,材料中含有要出国的团组信息、审批信息、团组成员的基本信息及出访地等信息,申报大厅的受理人逐一将基本信息输入到原有的系统。如果团组人员较多,则专管员需要一直在大厅窗口前排队等侯。这种操作方式大大增加了受理人员的工作量及专管员的等待时间,工作效率不高,所以很有必要开发一套既方便专管员填报工作,又能提高受理人工作效率的管理信息系统。

2 系统设计

我们灵活地采用 Web的 B/S架构与 C/S架构相结合的方式,既利用了 B/S结构在网络上优势,又兼顾了 C/S在操作上的便利性。

2.1 系统结构设计

根据需求分析,我们确定系统主要应该由申报客户端、外网服务器端、受理客户端三个功能模块组成。

2.2 网络拓扑

网络拓扑如图 1所示。

收稿日期:2006-11-22。宋兆辉,硕士生,主研领域:网络安全,信息处理。

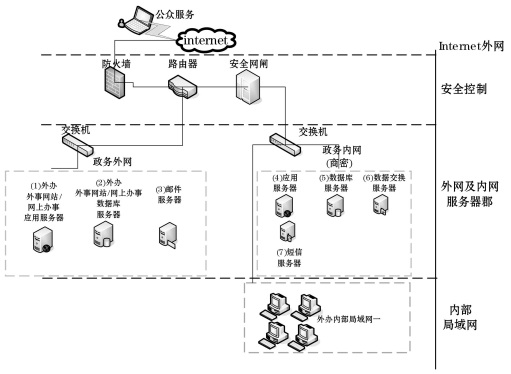

图 1　护照签证管理信息系统网络拓扑图

3　系统实现

3.1　基于安全网闸技术的内外网数据交换的实现

网闸(GAP)是一种快速、安全的网络物理隔离产品,采用物理隔离通道控制系统和嵌入式内核控制技术,以及多重安全措施,可以防止黑客攻击、病毒侵入和信息泄露等安全隐患,确保内网与外网的可靠隔离和信息的可靠交换。

基于网闸基本原理的内外网之间数据交换的体系结构如图2所示,其主要的工作处理流程如下:

1)外网(Internet)的各申报专管员通过申报客户端提交加密过的数据文件到受理中心的认证服务器上。

2)外网服务器对提交上来的数据进行验证,如果有错,则给出提示,否则,提示提交成功。

3)网闸外网监控模块通过专用通道,把外网机上的数据文件转到内网临时处理机上。

4)受理工作人员扫描条形码,把临时机上的数据调入正式机上并进行处理。

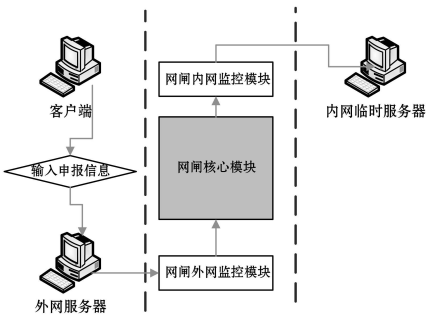

图　2

3.2　基于智能 key的远端身份安全认证

电子政务作为信息网络的一个特殊应用领域,运行着大量需要保护的数据和信息,相对于企业信息化和电子商务,有自身特殊性:一是信息内容的高保密性、高敏感度;二是电子政务发挥行政监督力度;三是利用网络环境为社会提供公共服务。如果系统的安全性被破坏,造成敏感信息暴露或丢失,或网络被攻击等安全事件,必然会产生严重后果。因此,对终端用户身份的安全认证就成为比较重要的一个问题。

目前常见的身份认证方式主要有三种:其中最常见的是用户名加口令的方式,但这也是最原始、最不安全的身份认证方式,非常容易由于外部泄漏等原因或通过口令猜测、线路窃听、重放攻击等手段导致合法用户身份被伪造;第二种是生物特征识别技术(包括指纹、声音、手迹、虹膜等),该技术以人体唯一的生物特征为依据,具有很好的安全性和有效性,但实现的技术复杂,技术不成熟,实施成本昂贵,在应用推广中不具有现实意义;第三种也是现在电子政务以及电子商务领域最流行的身份认证方式——基于智能 USB Key的身份认证。

MD5的全称是 message digest algorithm 5(信息-摘要算法),在 90年代初由 mit laboratory for computer science和 rsa data security inc的 ronald l. rivest开发出来,经 MD2、MD3和 MD4发展而来。它的作用是让大容量信息在用数字签名软件签署私人密匙前被"压缩"成一种保密的格式(就是把一个任意长度的字节串变换成一定长的大整数)。它可以对任何文件产生一个唯一的 MD5验证码,每个文件的 MD5码就如同每个人的指纹一样,都是不同的。这样,一旦这个文件在传输过程中,其内容被损坏或者被修改的话,那么这个文件的 MD5码就会发生变化,通过对文件 MD5的验证,可以得知获得的文件是否完整。

对 MD5算法可以简要的叙述为:MD5以 512位分组来处理输入的信息,且每一分组又被划分为 16个 32位子分组,经过了一系列的处理后,算法的输出由四个 32位分组组成,将这四个 32位分组级联后将生成一个 128位散列值。

智能 key是基于 MD5算法的硬件身份认证设备,其主要认证流程如图 3所示。

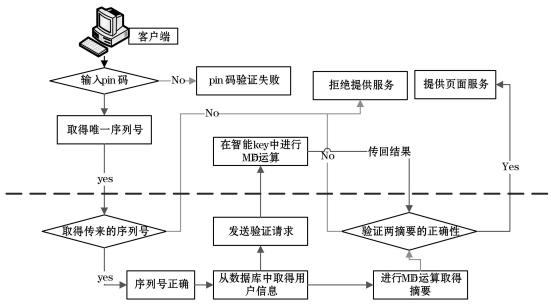

图　3

1)取得序列号　序列号可以是任何字符串或数字(如在数据库中的用户的账户或是智能 key的硬件 ID号),可以是用户输入的字符串,或是从智能 key中特定的文件中读出等,发送给服务器。

2)服务器发出验证请求　当服务器接收到客户机的序列号时,需要对序列号的真实性进行检查。因此,服务器开始对客户机的智能 key进行 MD5哈希信息码校验。要进行 MD5校验,服务器需要传递给客户机一个随机数,并且服务器必须记住这个随机数。

3)客户机响应服务器验证请求　将服务器传来的随机数传给智能 key,并在智能 key内部进行 MD5哈希信息码运算,从而得到 128位的摘要。这个摘要返回到服务器端。

4)服务器判断客户机的响应　服务器接收到客户机返回的摘要与序列号。根据序列号找到先前保存的随机数,和后台数据库中保存的用户持有的智能 key的硬件 ID号,以及智能 key中 MD5哈希信息码的内容。然后使用这些数据进行 MD5哈希运算,得到一个 128位的摘要。将这个摘要与客户机返回的摘要进行比较。相同则认为是合法用户,否则是非法用户。

4　结束语

安全问题是当前电子政务的核心问题,如何在保证安全的

(下转第 218页)

```
return <result> {book/title} {$book/market/sum} </result>
remainer_query for $book in doc("book_sale.xml")
    /book[publish>= 2005]
return <result> {$book/title} {$book/market/sum} </result>
```

子查询 probe_query可以直接被查询引擎 XQEngine在 result cache中 Q2对应的结果 XML文档上执行而获得结果，而 remainder_query则要根据元数据字典中各局部视图与全局视图的映射关系再次分解为对局部数据源视图 book.xml和 sale.xml的查询：

```
remain_q1 for $book in doc("book.xml")/book[publish>= 2005]
          return $book/bookId $book/title
remain_q2 for $sale in doc("sale.xml")/sale
          return $sale/bookId $sale/market/sum
```

假设 remain_q1和 remain_q2的查询结果分别为 bookTem.xml和 saleTem.xml，在结果合成部分形成最终查询 finally_query，再将查询结果返回给用户。

```
finally_query for $book in doc("book.xml")/book
    $sale in doc("sale.xml")/sale where $book/bookId =
$sale/bookId
return $book/title sale/market/sum
```

从以上实例可以看出，在网络环境下，上述的查询处理过程可以在本地获得部分查询结果甚至在某些情况下会获得全部结果，大大减少了本地与远程分布式数据源之间的信息传输量和查询响应的时间。

在采用面向对象编程思想设计多元变量树的结点类时，我们为其增加了如命中次数 N最近命中时间 T对应结果数据大小 M获取结果所花的时间△T等属性，这些属性被用于缓存替换策略 $R = w_1 \cdot N + w_2 \cdot T + w_3 \cdot M + w_4 / \triangle T$的计算，其中 w_i为参数的权值，对于不同数据源情况，这些权值也不尽相同。最后计算 R值，替换 R值最小的查询。

当语义区中保存的查询数量变大，要在众多查询中找到一个匹配的查询所花时间就不能忽略了。系统采用哈稀表管理缓存，Java5.0的新特性使 HashMap或 Hashtable支持泛性，因此可以将列表集合存储在哈稀表中，每个列表都存放对相同数据源的查询。当处理一个新的查询时，就可以根据该查询的数据源很快的找到它的候选匹配查询集，这就可以减少扫描缓存的时间。

对于缓存的一致性问题，系统采用自动刷新技术。当局部数据源表的字段或 XML文档结点有增删变化时，wrapper重新生成新的局部视图，注册到元数据字典中，系统删除原局部视图，更新全局视图，使其与各个数据源保持一致；如果是表或 XML文档中的数据有变化，则告知 Mediator产生变化的表名或 XML文档名，并在语义区中清空对该表或文档的缓存查询列表和 ResultCache中对应的查询结果。由于本文的方案主要针对数据规模大、并且更新不是很频繁的情况，故对系统的性能不会有太大影响。

3 实验分析

该模型的实验环境为 Windows2000+Eclipse+XQEngine，P4 3.00GHz内存为 512MB的 PC机 3台，其中一台作为服务器，另两台作为局部数据源。为了更好地观察嵌入语义缓存后系统性能变化同时也简化实验，我们用 XML文档集合（XQEngine自带的 XML格式的莎士比亚文集）作为实验的局部数据源。查询的响应时间 $T = T_{query_send} + T_{query_execution} + T_{result_return}$在 Web环境下，$T_{query_send}$和 T_{result_return}占据很大比率，如果使用缓存，在大部分情况下就能极大地减少甚至不需要这两部分的时间消耗。图 3显示了在使用缓存和不使用缓存两种情况下查询的响应时间比较情况。

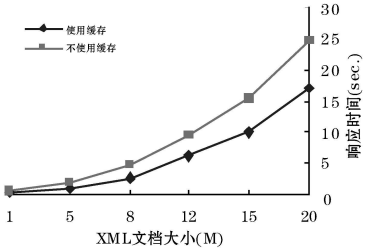

图 3 查询响应时间对比图

4 总 结

本文提出了一种在 Mediator-Wrapper结构中嵌入基于 XQuery语义缓存的异构数据集成的查询处理方案。实验数据表明，该方案能有效地提高信息集成系统的查询性能。

参 考 文 献

[1] Garden G, Mensch A, Dang-Ngoc T T, et al. Integrating Heterogenous Data Sources with XML and XQuery. Proceedings of 13th Internation Workshop on Database and Expert Systems Applications, 2002: 713-718.

[2] Wang Hongzhi, Li Jianzhong, He Zhenying. An Effective Wrapper Architecture to Heterogeneous Data Source. 17th International Conference on Advanced Information Networking and Applications: AINA 2003 (3): 565-568.

[3] Igor Tatarinov, Alon Halevy. Efficient Query Reformulation in Peer Data Management Systems. SIGMOD 2004 June 13-18, 2004.

[4] Gerome Miklau, Dan Suciu. Containment and Equivalence for an XPath Fragment. In Proceedings of the 21st ACM SIGACT-SIGMOD-SIGART Symposium on Principles of Database Systems, 2002: 65-76.

[5] Shaul Dar, Michael J Franklin, Björn T, Jónsson Semantic Data Caching and Replacement. Proceedings of the 22nd VLDB Conference Mumbai(Bombay), 1996.

[6] http://www.w3.org/TR/2005/CR-xquery-semantics-20051103/.

（上接第 193页）

前提下，使电子政务系统真正能便民、利民，简化政府审批程序，提高受理的工作效率，上海市人民政府外事办公室在这方面做了很多卓有成效的工作，取得了良好的效果。

参 考 文 献

[1] Kevin Gennuso. Disconnect from the Internet-Whale's-e-Gap Indepth. SANS Reading Room. [EB/OL]. https://www.sans.org/rr/whitepapers/firewalls/802.php. 2005.4.10.

[2] 双网隔离相关技术和方案. 网络技术论坛, Jul 20, 2005. http://bbs.s8s8.net/forums/lofiversion/index.php/t35252.html.

[3] Zeng K C, Yang J H, Dai Z D. Patterns of Entropy Drop of the Key in an S-box of DES. Advances in Cryptology-CRYPT'87. Spring-Verlag, 1988, 293: 438-444.