文章编号:1000 - 582X(2003)06 - 0042 - 03

企业信息集成平台电子文档安全存储管理技术*

王成良[1], 曾 德[2]
(1. 重庆大学 软件学院,重庆 400044; 2. 重庆大学 计算机学院,重庆 400044)

摘 要:企业在信息化过程中将会产生大量的电子文档。这些电子文档大多以磁盘文件方式分散存放在各个部门的计算机上。虽然可通过共享机制实现互访,但管理和维护较为困难,既产生信息孤岛问题,对重要敏感电子文档还会存在安全性问题。提出了将企业电子文档进行分类处理后以数据库方式进行存储管理、通过电子文档的授权访问机制以及对电子文档的加密、压缩处理后在网络上进行传输和存储的电子文档安全管理技术。通过在企业的实际应用表明,这种管理技术有效地实现了企业信息集成平台电子文档动态共享、查询方便、安全可靠的目的。

关键词:电子文档; 数据库; 授权管理; 加密; 压缩
中图分类号:TP311.11 **文献标识码**:A

随着信息技术的发展,企业大都建立了自己的信息集成平台。在该平台中存放着大量和企业发展密切相关的信息,例如市场调研报告、产品设计文档、各类零部件图形文档、质量检验报告、财务分析报告、员工培训与考核文档、重要会议记录、不合格品处理报告、产品订购合同、甚至重要讲话的录音、视频图像等多媒体信息。它们大都以各种电子文档的形式存在,其中包括着企业的许多重要敏感信息。如果将这些信息高效、安全地管理起来,即在保证敏感信息不被泄露的基础上,最大限度地让企业各类信息在其受限的范围内顺畅流动,发挥其最大效能,将极大地提高企业的运转效率,从而提高其竞争力。

当前企业电子文档的管理大多以目录文件的方式存放于企业相关部门的计算机或网络服务器上,通过设定的共享访问机制提供各级人员的访问或者通过将各个部门的电子文档上传到某一指定的计算机上供具有不同访问权限的工作人员进行访问。

上述目录文件的文档管理方式,虽具有一定的方便性,但对于现代企业来说,存在着以下问题:

1)电子文档分散存放在企业的信息集成平台中,要查询某一文档非常不便,费时费力,而且还有可能找不到;

2)直接以文件方式存放在磁盘中的电子文档,会因硬盘损坏而破坏;也容易因操作不当而被人为删除;如计算机受到病毒破坏,有可能使这些电子文档也受到破坏;

3)重要敏感文档甚至企业机密或绝密文档存在严重安全性问题。例如通过网上邻居或其它方式的文件目录共享,即使使用了一定的安全防范机制,但仍然可以较为容易地被窃取或遭到破坏[1];机密文档虽然已被删除,但有可能从磁盘中再行恢复出来;文档信息内容在网络传输过程中容易被截获和破解等[2-3]。目录文件方式的电子文档,虽然可对其进行加密处理来增强其操作安全性,但其安全性仍处于较低层次,并取决于操作系统的安全性,而操作系统的安全隐患较多。

为此笔者开发了一个企业电子文档安全管理系统 DocMgr,并已在企业中获得了较好的使用。基于 DocMgr 系统所用到的开发技术,下面从电子文档的存储管理、电子文档的授权管理以及电子文档的加密和压缩几个方面分别进行说明。

* 收稿日期:2003 - 09 - 11
基金项目:重庆市应用基础研究项目(20016809)
作者简介:王成良(1964 -),男,江苏丹阳人,重庆大学副教授,博士。主要从事网络及数据库应用技术研究。

1　电子文档的存储管理

对于电子文档的存储管理应采用数据库管理方式。将企业电子文档采用数据库方式进行管理除了具有查询快速方便；防止误删除；不会受病毒感染等优点外，对于企业重要、敏感文档通过数据库系统授权访问控制可提高其访问安全性，防止被窃取或遭到破坏。虽然目前关系型数据库对非结构化数据的处理功能比较薄弱，但大多数流行的关系型数据库如 ORACLE、SQL SERVER 等都支持对二进制大对象的存储，因此将电子文档用数据库方式来管理在技术上是切实可行的。此外，必须对企业电子文档进行分类管理。可以将企业电子文档按部门、管理性质、分属类别等进行分类管理存储。这种对电子文档层次的划分有效地将电子文档组织起来，当需要查询某个电子文档时，只要先选择其所属分类就可缩小查询范围，减少查询量，大大提高了查询效率，使得对存入数据库的电子文档的检索更为快速和简捷，从而有效地实现了企业电子文档分门别类的管理，也使得企业电子文档的授权管理变得容易。在 DocMgr 系统中采用了电子文档按部门的三级分类方式，如图 1 所示。

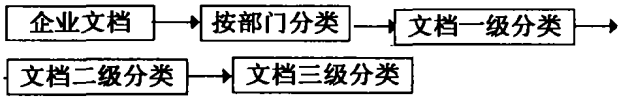

图 1　企业电子文档分类结构

2　电子文档的授权管理

企业中的电子文档不是所有人可以随意访问的，用户只能看到自己操作范围权限内的电子文档，因此对企业电子文档进行授权管理是必要的。有关授权访问的模型有很多[4-5]，但在 DocMgr 系统中，根据电子文档管理特点，采用了"管理授权"和"推荐式授权"来保证系统的安全性访问。其基本思想是：

1）用户始终属于某一个用户角色 R（User Role），由系统管理员 A（Administrator）为每个用户角色分配主体安全规则。[6]

2）根据权限作用的对象将权限分为功能型权限和实体型权限。某个用户角色对系统的访问分为功能型访问和实体型访问。功能型访问权限是指某用户角色是否具有使用电子文档数据库管理系统中某项功能的权力，例如某用户角色可以处理另外某部门的文档、可以进行用户定义、可以进行代码维护等就属于功能型访问权限；实体型访问权限是指用户角色访问特定的实体型对象的权力，如是否能够查看 B（Browse）、修改 M（Modify）、删除 D（Delete）、打印 P（Print）某个文档的权力。例如：某用户被授予了文档管理的权力，这就是一个功能型权限。拥有此权限就意味着用户可以使用文档管理模块的功能，但对某个具体的文档，如对某图纸、用户是否有查看、修改或删除该文档的权限就是实体型权限。

3）功能型访问的授权由系统管理员或子系统管理员来完成，称为管理授权，管理即是可以对企业中不同角色的员工进行划分，并依据角色给予其相应的功能授权。实体型访问的授权可以由系统管理员或子系统管理员，也可由文档所有人 DO（Document Owener）来完成，文档所有人可以根据用户而不是用户角色 UR 来确定其文档的操作权限，此过程称为推荐式授权。

4）从权限的有效性来看，可以将权限分为两类：固定权限和流动权限。固定权限是指各用户角色 R 拥有的权限，主要是指管理员授予的权限；流动权限是指因管理过程中用户因工作需要，文档所有者 DO（Document Owner）赋给其他用户的权限，如某用户 User1 承担某文档的设计任务，在文档获得签字认可后，用户 User1 有权让某用户 User2 进行查阅，此时用户 User1 可以进行推荐式授权，当然用户 User1 也可以收回对用户 User2 的文档管理权限。

5）对管理授权、推荐式授权有完整的日志审计功能，防止授权人将功能性权限和实体访问权限授予不相关的人。通过"管理授权"和"推荐式授权"，将整个文档管理系统的繁重的、动态的权限管理任务分解过来，大大减轻了人们的管理授权工作，使得系统的安全性大大提高，避免了由于授权滞后等各方面带来的安全问题。

3　电子文档的加密和压缩

在将本地电子文档存放到后台数据库之前，为了保证电子文档的安全性，应对电子文档进行必要的加密处理。从数据库取得电子文档后需要通过解密处理还电子文档的本来面目，以便人们查阅。

根据电子文档管理特点，电子文档的加密和解密无需用户干预，是一个动态加密和动态解密的过程，即保存到数据库前马上进行加密，从数据库取出后马上

进行解密,因此这类加密算法可设计得比较简洁,一般可采用对称加密算法。在 DocMgr 系统中,通过 Microsoft 提供的加密应用程序接口(即 Cryptography API),或称 CryptoAPI,采用了计算速度快捷的 DES 对称加密算法实现了电子文档的加密。

经过上述加密过了的电子文档如果不作数据压缩处理就存放到数据库中,一方面要引起数据库系统对磁盘空间存储需求的大量增加,另一方面延长了电子文档写入或读出数据库的时间,同时网络的传输量也会较大,使得网络上传输电子文档的时间增长,因此必须对电子文档进行压缩处理。

电子文档的压缩可以采用无损压缩方法例如哈夫曼压缩算法、LZW 压缩算法等等来实现。在 DocMgr 系统中,采用了 Xceed 软件公司提供的 Xceed Zip Compression Library v4.5ActiveX 控件来进行电子文档的动态压缩和动态解压。

5 结束语

通过将电子文档合理分类并且采用数据库进行管理,采用切实可行的电子文档授权访问管理以及电子文档的加密和压缩技术,将它们有机地结合起来,大大提高了企业电子文档的管理效率,实现了电子文档的安全存储管理。从已经使用 DocMgr 系统的企业反映的情况来看,使用灵活方便,效果良好。

参考文献:

[1] 郑辉,涂奉生. 网络邻居共享存在的安全隐患分析[J]. 计算机工程,2001,27(1):57-59.

[2] 邱保志,李向丽. Unix 系统的网络安全性[J]. 计算机应用,2000,20(2):48-50.

[3] 魏高. 网络的安全管理[J]. 科技情报开发与经济,2000,(2):33-35.

[4] 张晓辉,王培康. 大型信息系统用户权限管理[J]. 计算机应用,2000,20(11):36-39.

[5] 洪帆,余祥宣,倪晓俊. 多级安全 RDBMS 的安全策略[J]. 华中理工大学学报,1996,24(1):41-43.

[6] 李伟琴,杨亚平. 基于角色的访问控制系统[J]. 计算机应用,2000,20(2):16-22.

Secure Storage Management Technology of Electronic Documents on Information - integrated Platform in Enterprises

WANG Cheng-liang[1], *ZENG De*[2]

(1. Faculty of Software Engineering, Chongqing University, Chongqing 400044, China;
2. College of Computer Science, Chongqing University, Chongqing 400044, China)

Abstract: A great deal of electronic documents will be produced in enterprises, many of which in the form of disk files are stored in the computers of each department. Some are shared through the sharing mechanism, but they are difficult to manage and maintain. Security problems and information - isolated island may occur for some of these documents. A new technology of electronic document administration are introduced, in which authorized administration mechanism are taken and the documents are classified, encrypted, compressed and then transported via intranet and stored in database. Its application in enterprises has proved that documents can be shared and queried dynamically, conveniently and reliably by using the technology.

Key words: electronic document; database; authorized administration; encryption; compression

(编辑 吕赛英)