数字化档案馆中数据库安全策略探析

谢翠香

随着知识经济时代的到来，信息技术的飞速发展，档案馆作为我国信息资源中心之一,其数字化建设已经提上日程，档案馆的形态也发展到了数字档案馆这一高级阶段。如何有效地保证数据库系统的安全，实现数据的保密性、完整性和有效性，已经成为探索研究数字化档案馆的重要课题之一。

一、数据库安全性要求

1.数据库安全性的概念。数据库的一大特点是数据可以共享，但数据共享必然带来数据库的安全性问题。数据库的安全性是指保护数据库，防止因用户非法使用数据库造成数据泄露、更改或破坏。数据库系统的安全保护措施是否有效是数据库系统主要的性能指标之一。

2.数据库系统的安全性要求。从数据库安全性的概念来分析,设计一个安全的数据库必须实现数据的保密性、完整性和有效性。为了达到这些目标,我们必须考虑一系列的安全要求,使数据库安全得到保证。常见的安全性要求如表1所示。

表1 数据库的安全性要求

安全性要求	注释
物理上的数据库完整性	预防数据库数据物理方面的问题。如掉电，以及当被灾祸破坏后能重构数据
逻辑上的数据库完整性	保持数据的结构。例如:一个字段的值的修改不至于影响其他字段
可审计性	能够追踪到谁访问修改过数据库的元素
访问控制	允许用户访问被批准的数据，以及限制不同的用户有不同的访问模式，如读或写
用户认证	确保每个用户被正确地识别，既便于审计追踪,也为了限制对特定的数据进行访问
可获（用）性	用户一般可以访问数据库以及所有被批准访问的数据
保密性	以加密形式存储和传输

二、数字化档案馆中数据库总体安全策略

1.身份认证。为防止非法用户访问数据，在执行数据访问操作之前，要在客户和服务器之间进行身份验证。这是一个相当简单的过程，也是防止非法用户侵入的第一道防线，系统通过这个过程来证实用户身份。身份认证一般有三级：系统登录、数据库连接和数据库对象使用。系统登录一般由网络操作系统提供

档案史料是纺织服饰史研究的重要文献资料，但由于其大部分尚未公开出版，今人查阅具有一定难度，因而容易被研究者所忽略。希望类似本文的梳理工作可以引起更多人对档案史料的关注和重视；同时，也希望保存档案资料的机构可以为研究者提供更加便利、快捷的查阅平台。档

参考文献：

[1]中国第一历史档案馆.圆明园[M].上海：上海古籍出版社，1991

[2]中国第一档历史案馆.清代档案史料丛编·第五辑[M].北京：中华书局，1980

[3]中国第一历史档案馆编，中国社会科学院历史研究所译注.满文老档[M].北京：中华书局，1990

[4][清]孙 珮著.苏州织造局志[M].南京：江苏人民出版社，1959

[5]故宫博物院明清档案部.李煦奏折[M]北京：中华书局，1976

[6]故宫博物院明清档案部.关于江宁织造曹家档案史料[M].北京：中华书局，1975

[7]大清会典[M].北京：中华书局，1991

[8]嘉庆重修一统志[M].上海：上海书店，1984年重印商务印书馆1934年版

[9]松江府志[M].北京：书目文献出版社，1991

[10]张 謇.南通县图志[M].南京：南京大学出版社，1988

[11]朱雅娟.清代帝王服饰小样[M].紫禁城，1990(5)

[12]Asian Civilization Museum．Power Dressing[M].Singapore:2006

[13]故宫博物院.天朝衣冠——故宫博物院藏清代宫廷服饰精品展[M].北京：紫禁城出版社，2008

[14]黄能馥，陈娟娟.中华历代服饰艺术[M]．北京：中国旅游出版社，1999

（作者为上海纺织服饰博物馆博士/上海/200051）

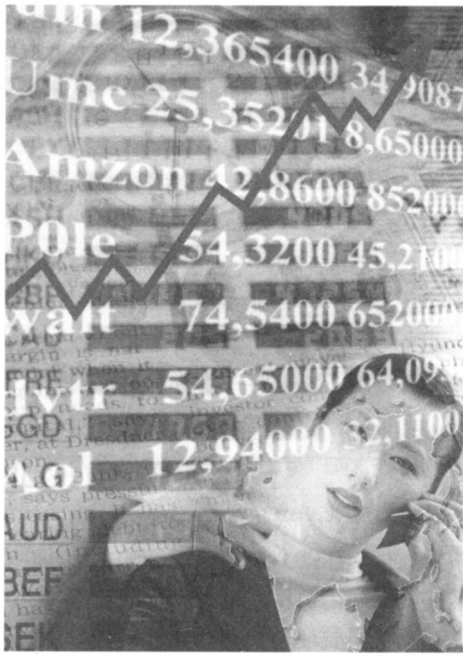
检查，要求用户输入用户名和口令加以验证。通过系统安全检查后用户才可以处理业务流程。当用户访问数据库时，就要求数据库管理系统验证当前用户身份是否可以进行数据库访问。在取得数据库登陆身份后，对数据库中的数据对象进行操作之前，数据库管理系统要再次检验用户对数据库对象的访问权限，以核实该用户是否有权对该数据库对象进行指定的操作。

2.存储访问控制。所谓访问控制，简单地说，就是对应保护的数据所进行的存取访问权限的确定、授予和实施。访问控制有两种形式：强制访问授权控制和自主访问授权控制。其中强制访问授权控制是指先给系统内的用户和数据对象分别授予安全级别，根据用户、数据对象之间的安全级别关系限定用户的操作权限。而自主访问授权控制由管理员设置访问控制表，此表规定用户能够进行的操作和不能进行的操作。数据的访问控制必须和用户的身份认证结合起来，才能形成有效的安全机制。

3.数据加密。数据加密是防止数据库中数据在存储和传输中失密的有效手段。数据加密的基本思想是，根据一定的算法将原始数据（术语为明文，Plain text）变换为不可直接识别的格式（术语为密文，Cipher text）。在传统的数据库系统中，系统管理员的权力至高无上，他既负责各项系统管理工作，例如资源分配、用户授权、系统审计等，又可以查询数据库中的一切信息。实现数据加密以后，各用户的数据由用户用自己的密匙加密，系统管理员获得的信息无法进行正常脱密，从而保证了用户信息的安全。

4.审计追踪。身份验证、存储访问控制和数据加密是目前信息系统设计中最为普遍的安全性方法，但目前的软件工程技术水平还无法证明或者保证任何一个系统不存在安全漏洞，也没有一种可行的方法，可以彻底解决合法用户在通过身份认证后滥用特权的问题。因而，一些信息系统中的大型DBMS提供的审计追踪便成了一个十分重要的安全措施。审计功能在系统运行时，可以自动对数据库的所有操作记录在审计日志中，以此来监视各用户对数据库施加的动作。若发现系统的数据遭到破坏，可以根据日志记录追究责任。

5.数据库的备份与恢复。计算机故障的原因多种多样，包括软件故障、电源故障、磁盘故障、人为破坏等。一旦发生这种情况，就可能造成数据库的数据丢失。数据库的备份与恢复是实现信息系统安全运行



的重要技术之一，是保证在数据库系统出故障时，能将数据库系统中数据恢复。加强数据备份非常重要，数据库拥有很多关键的数据，这些数据一旦遭到破坏后果不堪设想。一般的数据备份解决方案为以下三种：磁带备份、双机热备份、手工备份方法。

三、结语

档案馆与其他信息部门（如：图书馆）有较大的差异，其保管的数字信息并非完全对外公开，而是具有相应的密级。因此在数字档案馆的建设中，数字档案馆的安全保障体系建设成为首要考虑的问题。数据库系统的安全是数字档案馆安全保障体系的重要组成部分，也是数字档案馆正常运行的关键环节。为保障档案信息的真实性、完整性、可靠性、可用性，防范病毒与黑客的攻击，除了形成一套法规标准体系外，还需有相应的技术措施进行自动控制，在实际操作中可以采取上文所述的几方面安全策略，在设计数据库系统时做统筹安排，提高数据库中数据的安全性。档

参考文献：

1.张敏，徐震，冯登国．数据库安全．北京：科学出版社，2000.

2.卞咸杰．论档案信息安全保障机制的建立与完善．档案．2007，（6）：18-20．

3.王静．网络环境下的数据库安全综述．合作经济与科技．2009，（3）：38-39．

4. http://tech.csai.cn/dbms/tech20051102001.pdf

（作者单位：西北师范大学档案馆/兰州/730070）