

在计算机软件开发中数据库安全设计的应用实践

张颖忠

杭州云寰科技有限公司

DOI:10.12238/acair.v3i2.13551

[摘要] 在现今的信息时代,计算机软件开发技术已成为一股不可忽视的力量。网络的发展与深度改变了人类的资讯需要与信息来源。而数据库是计算机软件工作的中心,它的安全问题对整个软件的安全、对使用人员数据的安全都有很大的影响。但是,由于网络攻击方式的日益复杂化、复杂化,使得数据库受到了更大的安全风险。所以,强化数据库的安全性是计算机软件发展的关键。

[关键词] 计算机软件开发; 数据库; 安全设计

中图分类号: TU972+.4 **文献标识码:** A

The application practice of database security design in computer software development

Yingzhong Zhang

Hangzhou YunhuanTechnology Co., LTD.

[Abstract] In today's information age, computer software development technology has become a force that can not be ignored. The development and depth of the network has changed the need and source of human information. And the database is the center of the computer software work, its security problems on the security of the whole software, the security of the use of personnel data have a great impact. However, due to the increasing complexity and complexity of the network attack mode, the database is subject to greater security risks. Therefore, strengthening the security of the database is the key to the development of computer software.

[Key words] computer software development; database; security design

近年来,互联网技术得到了长足的发展,各种计算机技术也被越来越多地应用到了各个领域,而在计算机技术与时代的快速发展相互结合、相互冲击的过程中,也相继诞生了一批高科技产品,最为典型的莫过于计算机软件开发中的数据库安全设计技术,这些先进的技术给国内的计算机软件开发工作提供了更多的机会与挑战,将数据库安全设计技术引入到国内计算机软件的研发当中,既可以加速国内计算机软件的研发速度,又可以促进国内的高端科技的持续发展,从而推动国家的长远发展。

1 计算机软件开发和数据库概述

1.1 计算机软件开发

随着科技的飞速发展,互联网计算机的应用越来越广泛,也越来越深刻地改变着我们的生产和生活。尤其是对大多数人来说,在计算机技术的大力支撑下,移动电话等智能终端已经逐渐融入到我们的日常生活中,给日常生活带来了巨大的方便。但是总体上来说,整个程序设计较为困难,不仅要求对多种程序语言的精通和使用,还由于软件的发展离不开多种多样的软件开发环境,因此具有一定的挑战性。工作人员在进行详细而又繁杂的计算机软件开发工作时,要使软件数据得到科学、有效地处理,给使用者更加准确的服务,就需要进行相关的数据库的撰写。唯

有如此,方能更好地保护使用者的基本权益,以适应广大客户的多元化需要。

1.2 数据库

数据库是一种根据数据结构对数据进行组织、存储和管理的一种仓储。数据库是企业管理,电子商务,财务管理的重要组成部分。数据库可以帮助用户高效地存储、检索和处理数据,广泛应用于企业管理、电子商务、金融等领域。数据库是根据特定的数据模型来进行组织与储存的一种数据。DBMS是对数据库进行管理的一种程序,为数据定义、操作和控制等方面的实现。通过SQL与DBMS进行互动,完成对数据的查询、插入、更新、删除等功能。另外,在软件开发过程中,也要对其进行测试,以避免在以后的应用中由于性能问题而导致的安全风险。如果用户在使用过程中不慎下载了不明链接,导致计算机遭受病毒侵害,这将严重威胁到数据库的安全,影响其中存储的数据信息。因此,技术人员必须对数据库的性能测试给予高度重视^[1]。详细的测试步骤如图1所示

2 计算机软件开发中数据库安全设计

2.1 科学设置用户权限

一方面,要保证数据库的安全、有效地运作,就必须对数据

库中的使用者与使用者进行明晰化,这是对以后授权资源进行有效配置的关键环节。特别是,对于那些真正想要存取数据库的使用者或使用团体,应该加以谨慎的鉴别,并且还要决定他们应该拥有的作业权利的范畴,其中包括读取数据、写入数据、修改数据、删除数据、建立表格等基础操作。同时,应与使用者的真实需要以及他们所承担的任务密切相关,为他们准确地赋予适当的权力,保证每个使用者只能对自己工作需要的特定物体进行存取和操纵,例如特定的视图、存储过程等。

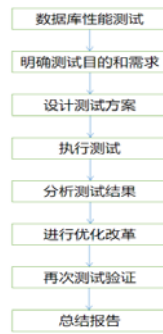


图1 数据库性能测试步骤

另一方面,为了持续提升数据库的安全性,还必须建立并实施一套定期审查和更新权限设置的机制。该机制的目的是保证数据库的权限分配与商业发展的现实需要密切相关,并且在一定程度上符合已建立的安全性规范。另外,针对不同的使用者,通过对其进行个性化的授权与授权,可以对其进行精细的管理,从而更好的减少系统的隐患。例如,您可以将最高级的授权授予数据库管理员,让他们对整个数据库系统进行完整的管理;而对一般使用者,仅给予较低级的使用权限,并将其存取数据库和使用权限加以严密控制,以加强数据库的安全性^[2]。

2.2 数据库自动化处理设计

(1) 自动化备份任务: 设置定期的自动备份工作,依据数据的重要程度及变动次数决定备份时间,例如每日、每周或按月完整备份,或按小时备份或半日备份。为避免局部灾害(如火灾、地震等)造成的损失,需要将其分散存放于多个地理空间,如分布式的数据中心或云端服务器。(2) 自动化监控与报警: 通过数据库管理系统的监测手段或者第三方监测程序,实现对数据库的各项性能参数(CPU利用率、内存利用率、磁盘 I/O等)、连接数、出错日志等的监测。在一些特定的参数超出预先设定的临界值时,会产生警报,提醒数据库管理者进行相应的处置,以防止由于系统失效或执行不当而对数据库的安全造成威胁。(3) 自动化恢复流程: 建立全面的自动化恢复方案与脚本,以保证在数据库发生故障或数据遗失的情况下,能够迅速且精确地恢复数据。通过执行测试和模拟,检验恢复流程的实用性和效率,降低恢复时间目标(RTO)和恢复点目标(RPO),减轻数据损失和业务中断的不良影响^[3]。

2.3 应用数据加密技术

2.3.1 静态数据加密

(1) 文件级加密: 假设数据库文件为 F , 加密函数为

$E_K(F)$, 其中 K 是密钥。解密函数为 $D_K(E_K(F))$, 且满足

$D_K(E_K(F)) = F$ 。这种加密方式确保了整个数据库文件在

存储时是安全的。(2) 列级加密: 对于数据库中的特定列 C_i ,

加密函数为 $E_{K_i}(C_i)$, 其中 K_i 是针对该列的密钥。解密函数为

$D_{K_i}(E_{K_i}(C_i))$ 。这种加密方式可以实现更细粒度的安全控制,

例如,对于包含用户敏感信息的列进行加密存储。

数学上,这种加密方式通常基于对称加密算法,如AES(高级加密标准),其安全性依赖于密钥的复杂性和算法的安全性。AES加密可以表示为:

$$C = E_K(P)$$

其中 P 是明文, C 是密文, K 是密钥。解密过程为:

$$P = D_K(C)$$

2.3.2 动态数据加密

在数据传输过程中,使用安全的传输协议,如SSL/TLS,进行加密。SSL/TLS协议基于公钥基础设施(PKI),使用非对称加密算法(如RSA或ECC)进行密钥交换,然后使用对称加密算法(如AES)进行数据加密。

假设发送方为 A , 接收方为 B , 公钥为 PK_B , 私钥为

SK_B , 会话密钥为 K_S 。密钥交换过程可以表示为:

$$K'_S = E_{PK_B}(K_S)$$

其中 K'_S 是加密后的会话密钥。接收方 B 使用私钥 SK_B

解密得到会话密钥 K_S :

$$K_S = D_{SK_B}(K'_S)$$

然后,双方使用会话密钥 K_S 进行对称加密通信。

2.3.3 密钥管理

密钥作为信息安全的重要组成部分,必须对其进行严密的安全管理。密钥的产生,储存,分发,使用和销毁都要按照一定的安全性标准进行。为了避免由于密码的泄漏而造成的密码失败,需要经常对其进行替换,并将其存放在诸如硬件保密模组(HSM)等安全位置^[4]。

2.4 备份与恢复

通过设计一个良好的备份方案,灵活使用全量备份、增量备

份和差别备份等备份方式,可以显著提高企业在面临数据损失和破坏时的应变能力。全量备份,顾名思义,是对所有数据进行的完整复制,为客户提供了数据的全面快照,方便在灾难发生时对数据进行全面恢复。同时,增量备份只针对上一次备份后发生变化的数据部分,只对添加或者更改过的数据进行备份,这样既节约了内存,又节约了备份的时间。差异备份是中间的一种,对最后一次全量备份之后更改过的所有数据进行备份,虽然与增量式备份比起来,它还包括了以前没有做过的、没有做过修改的数据,但是由于仅需要一个完整的备份加一个最新的差别备份,所以还原起来更加容易。为了保证备份数据的安全性,需要将备份文件存放在一个与产品环境完全隔离的地方,例如,为了避免局部灾难对备份数据造成损害。在此基础上,将数据存储的全流程进行自动处理,大大减轻了数据存储的工作量,同时也增加了数据的可靠性和时效性^[5]。

3 计算机软件开发中数据库安全设计的应用

3.1 提升数据库自动化处理能力

目前,在计算机软件的研究开发中,不仅要数据库的存储与处理数据信息的能力给予足够的关注,保证系统能够对大量的数据进行高效准确的处理,还必须着重提高数据库中的信息的安全与实时性,以便能够有效地防范数据泄漏,保证数据的适时更新。因此,在开发过程中,工程师必须充分利用云计算技术的强大优势,构建方便高效的交互渠道,从而提高整个软件的总体性能与使用效率。而大量的使用者,也能通过这个高技术的系统,轻易地享用到各种轻松享受到自动化数据处理所带来的种种便利和优势。同时,研发人员还需密切与BDS自动控制技术相融合,深入地对数据处理过程进行深入的优化与完善,从而提高数据处理的效率与精度^[6]。

3.2 建立信息安全管理平台系统



图2 信息安全管理平台系统

信息安全管理平台系统(如图2)集成了身份认证、访问控制、数据加密、日志审计等多重安全机制,为数据库提供全方位的安全防护。采用严谨的认证过程,保证了仅经授权的使用者可

以存取机密数据。并且,针对不同使用者的不同身份与不同的使用权限,进行不同程度的管控,以达到避免数据外泄的目的。而数据的密码学,是将机密数据储存与传送的密码,使得数据在未经授权的情况下,很难破译。通过日志审核,将整个数据库的运行情况全部记录下来,方便对安全事故进行跟踪和研究。该平台的建成将大大提高数据库的安全性,为实现该软件的安全性奠定坚实的基础。

3.3 定期更新维护操作系统

操作系统是整个数据库运作的基础,它的安全状况对整个数据库的保护有很大的作用。随着计算机网络的发展,各种新的网络攻击与攻击也随之出现,使得对系统进行实时升级,并对其进行相应的修复已是一种有效的防御措施。通过对现有的安全缺陷进行周期性的升级与修补,能够有效地解决现有的安全缺陷,提高系统的防护水平。此外,在日常的系统维修过程中,还需要对数据库执行性能的调整,以及多余的数据的清除,从而保证其有效、可靠地工作。另外,通过对系统进行周期性的安全检测与评价,能够对系统中存在的各种风险进行检测和解决,对于保证系统的安全性具有重要意义^[7]。

4 结论

总之,在计算机软件开发过程中实施数据库安全设计,对于提升开发效率、确保软件基础质量以及推动软件开发的持续健康发展,都具有极其重要的意义。

[参考文献]

- [1]王振华.计算机软件开发中数据库安全设计的应用实践分析[J].信息记录材料,2023,24(08):125-127.
- [2]任蕾蕾.计算机软件开发中数据库安全设计研究[J].网络安全和信息化,2023,(03):55-57.
- [3]顾正瑶,袁荣成.计算机软件开发中数据库安全设计的应用研究[J].长江信息通信,2022,35(11):148-150.
- [4]陈中凯.试论在计算机软件开发中数据库安全设计的应用实践[J].信息系统工程,2020,(12):119-120+122.
- [5]平金珍,王茜.计算机软件开发中数据库安全设计的应用实践分析[J].电子元器件与信息技术,2020,4(05):34-35+42.
- [6]贾斌,代云皓.试论在计算机软件开发中数据库安全设计的应用实践[J].电脑知识与技术,2020,16(09):1-2.
- [7]陈红艳.试论在计算机软件开发中数据库安全设计的应用实践[J].河北农机,2019,(06):48-49.

作者简介:

张颖忠(1967--),男,汉族,四川省绵阳市三台县人,本科,中级,杭州云寰科技有限公司,研究方向: 算机软件开发,人工智能、大数据、嵌入式开发。