计算机数据库的安全防范措施探究

葛瑞雪[1] 王晶晶[2] 程鸿帅[3]
1. 南水北调中线信息科技有限公司 北京 100038
2. 南水北调中线信息科技有限公司 北京 100038
3. 中国南水北调集团中线有限公司 北京 100038

摘 要：计算机数据库安全防范需构建多层次防护体系。技术层面，通过静态与动态数据加密、RBAC/ABAC权限管理、SSL/TLS传输加密及AES/RSA算法保障数据保密性；实施实时审计日志、SIEM系统集成及AI入侵检测强化监控能力。管理层面，制定全生命周期安全规范，定期开展分层安全培训，结合物理环境防护如多道门禁、温湿度监控与灾备方案。新兴技术方面，零信任架构与区块链技术进一步提升安全韧性。

关键词：计算机；数据库；安全防范措施

引言：在数字化浪潮席卷的当下，计算机数据库作为信息存储与处理的核心，承载着海量关键数据，涵盖个人隐私、企业机密乃至国家安全信息。然而，数据库面临诸多安全威胁，如外部黑客攻击、内部人员违规操作、软件漏洞利用等，这些威胁时刻威胁着数据的保密性、完整性与可用性。深入探究计算机数据库安全防范措施，构建坚实的安全防护体系，成为保障数据安全、维护业务稳定运行的迫切需求与关键课题。

1 计算机数据库安全概述

1.1 数据库安全的基本概念

（1）定义与内涵：数据库安全指通过技术、管理等手段，保障数据库中数据的保密性、完整性与可用性。保密性要求仅授权用户可访问敏感数据，防止信息泄露；完整性确保数据在存储、传输和使用中不被未授权篡改、破坏，保持准确性与一致性；可用性则保证授权用户在需要时能正常访问和使用数据库服务，避免因故障、攻击等导致服务中断。（2）数据库安全威胁类型：包括外部攻击，如黑客利用网络漏洞入侵数据库窃取数据；内部泄露，即内部人员因疏忽或恶意泄露敏感数据；管理漏洞，如缺乏完善的安全管理制度、权限分配混乱、未及时更新安全补丁等，均会给数据库安全带来风险。

1.2 数据库安全的核心目标

（1）防止未授权访问：通过身份认证、权限控制等机制，严格限制用户访问范围，杜绝未经许可的用户或超出权限的用户获取数据库数据，保障数据访问的合法性。（2）保障数据完整性：采用数据校验、加密存储、日志审计等技术，实时监控数据状态，及时发现并阻止对数据的非法篡改，确保数据始终处于准确、完整的状态。（3）确保业务连续性：建立数据库备份与恢复机制，应对设备故障、自然灾害、网络攻击等突发情况，减少服务中断时间，保障基于数据库的业务能够持续稳定运行[1]。

1.3 常见数据库安全威胁分析

（1）SQL注入攻击：攻击者通过在应用程序输入框中插入恶意SQL语句，利用程序对输入验证不严格的漏洞，非法执行SQL命令，获取、篡改数据库数据甚至控制数据库服务器。（2）跨站脚本攻击（XSS）：攻击者将恶意脚本代码注入到网页中，当用户访问该网页时，脚本代码在用户浏览器中执行，可窃取用户Cookie、会话信息等，进而间接威胁数据库安全。（3）数据库漏洞利用：数据库软件自身存在的漏洞，如缓冲区溢出漏洞，攻击者可利用该漏洞向数据库服务器发送特制数据，触发漏洞并执行恶意代码，获取服务器控制权。（4）内部人员滥用权限：内部员工利用自身拥有的数据库访问权限，超出工作需求获取、泄露敏感数据，或恶意篡改、删除数据，对数据库安全造成严重威胁。（5）物理环境风险：数据库服务器所在物理环境若遭遇火灾、洪水、地震等自然灾害，或服务器硬件设备出现故障、被盗等情况，会直接导致数据库数据丢失或服务中断。

2 计算机数据库安全防范技术

2.1 访问控制技术

（1）身份认证机制：多因素认证结合密码、动态验证码、硬件令牌等多种验证方式，大幅提升身份核验安全性；生物识别技术如指纹、人脸、虹膜识别，利用个人生物特征的唯一性，避免身份信息被盗用，为数据库访问筑牢第一道身份防线。（2）权限管理：RBAC（基于角色的访问控制）模型按用户角色分配预设权限，简

化权限管理流程，减少权限分配混乱；ABAC（基于属性的访问控制）模型依据用户属性、环境属性、资源属性动态判断访问权限，适配复杂业务场景下的精细化权限管控需求。（3）最小权限原则的应用：仅为用户分配完成工作必需的最小权限，避免多余权限带来的安全风险，例如普通员工仅拥有数据查询权限，无数据修改或删除权限，从权限源头降低数据泄露、篡改风险。

2.2 数据加密技术

（1）静态数据加密：对数据库文件、备份数据等静态存储的数据进行加密处理，即使存储设备被盗或数据被非法拷贝，未获取密钥也无法解读数据，常见方式包括数据库透明加密、文件系统加密。（2）动态数据加密：采用SSL/TLS协议对数据库与应用程序、用户终端之间传输的数据进行加密，防止数据在传输过程中被窃听、篡改，确保数据从源头到数据库服务器传输过程中的安全性，避免传输链路中的数据泄露[2]。（3）加密算法选择：AES（高级加密标准）算法安全性高、运算效率优，适用于大量数据加密，常用于静态数据与动态数据加密；RSA算法基于非对称加密原理，可用于密钥交换、数字签名，在加密密钥传输场景中广泛应用，二者结合可兼顾加密安全性与实用性。

2.3 数据库审计与监控

（1）日志审计技术：记录数据库的访问操作、权限变更、数据修改等所有行为日志，包括操作时间、操作账号、操作内容等信息，日志数据长期留存，便于事后追溯安全事件根源，例如通过审计日志可快速定位数据篡改操作的执行主体。（2）实时行为监控与异常检测：实时跟踪数据库访问行为，建立正常行为基线，当出现异常操作如高频次数据查询、非工作时间的敏感数据访问时，及时触发告警，帮助管理员快速发现潜在安全威胁。（3）SIEM（安全信息与事件管理）系统集成：将数据库审计日志、监控数据与SIEM系统对接，实现多源安全数据的集中分析、关联挖掘，通过系统自动识别安全事件关联关系，提升安全事件的检测与响应效率，例如将数据库异常访问与网络攻击日志结合分析，精准识别入侵行为。

2.4 数据备份与恢复技术

（1）定期备份策略：全量备份对数据库所有数据进行完整备份，备份数据全面但耗时较长，适合每周或每月定期执行；增量备份仅备份自上次备份后新增或修改的数据，备份效率高，适合每日执行，二者结合形成“全量+增量”的分层备份体系，平衡备份完整性与效率。（2）异地容灾与快速恢复方案：在异地建立容灾备份中心，将本地备份数据同步至异地，应对本地遭遇自然灾害、设备损毁等极端情况；制定快速恢复方案，明确恢复流程、责任人与时间目标，例如通过预配置恢复环境、使用快照恢复技术，将数据恢复时间缩短至分钟级，减少业务中断损失[3]。

2.5 新兴技术应用

（1）人工智能在入侵检测中的应用：利用AI算法对海量数据库访问数据进行学习，识别复杂、隐蔽的入侵模式，如异常数据访问序列、新型SQL注入变体，相比传统检测方法，提升入侵检测的准确性与时效性。（2）区块链技术保障数据不可篡改性：将数据库关键数据的哈希值存储于区块链，区块链的去中心化、链式存储特性确保哈希值不可篡改，若数据库数据被篡改，通过比对区块链中的哈希值可快速发现，适用于金融、医疗等对数据完整性要求极高的场景。（3）零信任架构（ZeroTrust）的实践：遵循“永不信任，始终验证”原则，无论用户处于内部还是外部网络，访问数据库时均需经过严格身份认证与权限校验，通过微服务化数据库访问接口、动态权限调整，构建全方位的数据库安全防护体系。

3 计算机数据库的安全防范措施

3.1 安全管理制度建设

（1）制定数据库安全规范与操作流程：需结合业务场景与数据敏感等级，明确数据库全生命周期的安全要求。例如，规范数据录入时的格式校验标准、敏感数据查询的审批流程、数据库补丁更新的操作步骤，如更新前需进行备份、测试环境验证，同时明确故障应急响应流程，如数据泄露后需在规定时间内启动溯源、止损、上报等操作，避免因操作无序扩大安全风险。此外，制度需定期修订，适配新的数据库技术，如云数据库与安全威胁，如新型勒索攻击，确保规范的时效性与适用性。（2）定期安全培训与意识提升：针对不同岗位人员制定分层培训计划。对数据库管理员，重点培训漏洞修复、审计日志分析、应急处置等技术技能；对普通员工，聚焦数据安全意识，如识别钓鱼邮件避免账号泄露、不随意分享数据库访问权限等。培训形式可结合案例教学，如展示内部人员滥用权限导致的数据泄露事件、模拟演练，如模拟SQL注入攻击场景，让员工实操防御，并通过定期考核，如安全知识测试、实操评估检验培训效果，将安全意识融入日常工作习惯，减少人为失误引发的安全风险[4]。

3.2 人员安全管理

（1）权限分级与职责分离：依据“最小权限+按需

分配”原则，对数据库访问权限进行分级。例如，将权限划分为超级管理员，负责数据库整体配置、运维人员，负责备份、补丁更新、业务人员，仅拥有特定业务数据的查询权限，避免单一人员掌握过高权限。同时，推行职责分离制度，如数据录入与数据审核由不同人员负责、数据库运维与安全审计由不同团队承担，形成相互监督、相互制约的机制，防止因“一人多职”出现权限滥用或操作失误无法追溯的问题。（2）离职人员权限回收机制：建立“离职流程-权限核查-回收确认”的闭环管理体系。在员工离职前，人力资源部门需及时通知IT部门，IT部门通过权限管理系统核查该员工的数据库访问权限，包括账号、密钥、临时授权，并在离职当日完成权限冻结与回收。对于核心岗位人员，如数据库管理员，还需变更相关敏感信息，如数据库管理员密码、密钥、审计其离职前一段时间的操作日志，排查是否存在数据泄露或恶意操作风险。同时，留存权限回收记录，如回收时间、操作人、回收内容，便于后续审计追溯，避免因权限回收不及时导致的安全隐患，如离职人员利用未回收的账号访问数据库。

3.3 物理环境安全

（1）数据中心访问控制：采用“多道防线”管控数据中心入口，第一道为园区门禁，通过刷卡+人脸双重认证；第二道为机房门禁，仅允许数据库管理员、运维人员等授权人员进入，且需登记访问事由与时间；第三道为服务器机柜门禁，采用指纹解锁，记录每一次开启操作。同时，数据中心安装24小时监控摄像头，覆盖出入口、机柜区域，监控录像留存至少3个月，便于事后追溯。（2）设备防盗与防破坏措施：数据库服务器需固定在机柜中，机柜加装防盗锁，重要设备粘贴防拆标签，一旦被拆卸即触发告警。针对自然灾害与环境风险，数据中心配备UPS不间断电源，确保断电后仍能维持服务器运行1小时以上，为数据备份争取时间；安装温湿度传感器与消防系统，当温度超过30℃或湿度高于80%时自动报警，火灾时采用气体灭火，避免水灭火损坏设备。此外，定期对服务器硬件进行巡检，排查硬盘故障、线路老化等问题，减少设备自身故障导致的安全风险[5]。

3.4 合规性与标准遵循

（1）国内外安全标准：针对境外业务或涉及境外用户数据的场景，需遵循GDPR（《通用数据保护条例》）要求，例如获取用户数据时需明确告知用途，用户有权要求删除个人数据，数据传输至境外需经过合规评估。针对国内业务，需符合等保2.0（《信息安全技术网络安全等级保护基本要求》），根据数据库重要程度确定保护等级（如金融行业数据库多为三级或四级），按等级要求部署访问控制、审计、备份等安全措施，并定期通过第三方测评机构的等级保护测评。（2）法律合规风险应对：建立合规风险排查机制，每半年由法务部门联合IT部门对数据库系统进行合规检查，重点排查是否存在数据收集不规范、敏感数据未加密、日志留存不足等问题，提前整改隐患。同时，制定法律纠纷应对预案，若发生数据泄露等合规事件，第一时间启动应急响应，通知受影响用户，向监管部门报告，并委托专业律所评估法律责任，避免因应对不当导致处罚升级（如GDPR最高可处全球年营业额4%的罚款）。此外，定期组织员工学习《数据安全法》《个人信息保护法》等法律法规，确保操作符合法律要求，从源头降低合规风险。

结束语

计算机数据库安全防范是场持久战，关乎数据资产安全与业务稳定发展。本文从技术、管理、物理环境及合规等多维度展开探讨，虽提出诸多防范措施，但安全威胁不断演变，新的漏洞与攻击手段持续涌现。未来，需持续关注前沿技术发展，如量子加密等，完善安全管理体系，强化人员安全意识。唯有不断优化、创新防范策略，才能构建起坚不可摧的数据库安全防线，为数字化时代的信息安全保驾护航。

参考文献

[1]郭新明.计算机数据库的安全防范措施分析[J].数码设计,2021,10(1):24-25.

[2]蔡南发,骆斌.计算机数据库的安全防范措施核心探究[J].福建质量管理,2020(12):65-66.

[3]武治国.刍议计算机数据库的安全防范措施[J].中国科技信息,2021(23):84-85.

[4]高蕾,索剑.计算机数据库安全防范措施的构建研究[J].电子技术与软件工程,2020(19):251-252.

[5]寿晓华.试论计算机数据库的安全防范对策[J].内蒙古科技与经济,2021(09):70-71.