数据管理中计算机科学技术运用分析

王晨盛

四川大学计算机学院，四川成都，610065；

摘要：在社会发展中，各行业每天都会产生海量的数据，那么就要对这些数据进行高效的管理和利用，满足社会发展对数据的需求。文章主要运用计算机科学技术，提出了实现数据加密管理、加强数据风险评估、开展数据风险预警、实现数据备份管理、增强数据访问控制等数据管理方法，保证数据管理更全面，增加了数据的价值，使得数据运用更加安全。

关键词：数据管理；计算机科学技术；风险预警

DOI：10.69979/3041-0673.25.08.020

引言

随着互联网、移动设备的普及，使得数据量逐渐呈指数级增长，传统的数据管理方法已经无法应对这一海量的数据资源，那么就要采用计算机科学技术。通过计算机科学技术对数据进行加密、风险预警、备份等管理，保证数据管理的效率得到提升，进而为企业提供更加精准的决策支持，提升了企业发展的竞争力。

1 计算机科学技术在数据管理中的作用

在数据管理中，计算机科学技术主要扮演着至关重要的角色，它不仅可以改变了传统数据管理的方式，还极大的提升了数据存储、处理和共享的能力。

第一，计算机科学技术实现数据储存与管理。计算机科学技术中的关系型数据库和非关系型数据库，就为数据提供了存储空间，保证数据储存和查询能力得到提升，同时，此技术也支持对结构化数据和非结构化数据进行存储，进而满足了多样化的业务需求。在数据储存的时候，也可以采用分布式文件系统和分布式数据库，进而实现了对海量数据的存储和容错处理，让数据储存管理能力得到提升[1]。

第二，计算机科学技术实现了数据处理。在数据处理时，使用 Hadoop、Spark 等框架，就能实现对海量数据的分布式处理和并行计算，并且支持对实时数据流进行处理，满足各行业对数据进行实时分析的需求。在数据处理的时候，通过 ETL 工具，能够对数据进行清洗、转换和整合等方面的处理，进而提高了数据处理的质量，并从数据中提取到一些有价值的信息，支持后续的数据预测和决策。

第三，计算机科学技术也能实现数据可视化效果。数据管理人员使用 Tableau、Power BI 等工具，就可以将复杂的数据以图表、仪表盘等形式，直观的展示出来，并为人员提供交互式数据的探索功能，帮助用户可以快速发现数据发展趋势。

第四，计算机科学技术能够实现数据安全与隐私保护。在采用计算机科学技术的时候，人员可以使用对称加密技术和非对称加密技术，来保护数据自身的机密性。也可以通过角色权限管理、访问控制技术，进而限制了数据的访问权限，保证数据隐私得到保护，降低了数据泄露等问题。随着技术的不断进步，计算机科学技术也将继续推动数据管理向更智能、更安全、更高效的方向稳定发展。

2 数据管理运用计算机科学技术的要点

2.1 实现数据加密管理

在进行数据管理中，数据保护是管理的重要内容，所以就要运用计算机科学技术，对数据开展加密管理，进而可以保证了数据的机密性、完整性和安全性。进行数据加密管理，可以防止一些未经授权的用户来访问敏感数据；也可以防止数据在传输或存储的过程中被恶意的篡改，进而提升了数据的真实性。在选择加密技术的时候，一是选择对称加密技术，主要是使用 AES，设计出相同的密钥，进而对大量的数据进行加密和解密，其加密性能比较高。二是选择非对称加密技术，主要是使用 RSA、ECC 等技术，实现公钥加密、私钥解密的效果，进而保证密钥交换和数字签名等数据更加安全。三是选择哈希算法，可以将数据转换为固定长度的哈希值，通过哈希值来验证了数据的完整性，保证数据加密更高效。四是选择混合加密的方法，把对称加密和非对称加密结

合使用，可以先用非对称加密技术来交换密钥，再用对称加密技术来传输数据，使得数据的储存、使用更加安全[2]。

在开展数据加密管理时，管理人员需要先根据数据的敏感程度，对其进行分类，确定需要加密的数据范围。然后就要根据不同的数据类型进行加密，先是文件级的加密，然后就要对数据库中的特定字段进行加密，接下来就要对整个磁盘进行加密，最后就是对传输中的数据进行加密。通过分层加密，能够保证数据加密更高效。在数据传输过程中进行加密的时候，可以使用 SSL/TLS 协议，对网络传输数据进行加密，防止数据在传输过程中被窃取或篡改。在数据存储时，则是要对存储在数据库、文件系统或云存储当中的数据进行加密。通过科学的加密管理，可以使的数据更加完整、隐秘，进而保障了数据自身的安全性。

2.2 加强数据风险评估

在进行数据管理时，为了保证数据的安全，那么就要对数据风险进行评估，进而有效识别了数据的资产和价值，分析出潜在的数据安全威胁，保证数据的使用更安全。在运用计算机科学技术进行数据风险评估的时候，先要列出数据库、文件、应用程序、云存储等区域中的所有数据资产，然后就要根据敏感性和重要性对数据进行分类，主要是分为公开数据、内部数据、机密数据等类型。同时，管理人员也要追踪数据在系统内的流动路径，明确了数据存储、传输和处理的关键节点。接下来，就要开展威胁识别，主要是识别出造成数据风险的因素，因素分为内部危险以及外部危险，其中内部威胁主要是员工的误操作、员工恶意行为或权限滥用等。外部威胁则是网络攻击、恶意软件、数据泄露等方面。通过对这些危险进行识别，可以了解数据风险的主要原因，并对其进行防护管理。在数据风险识别完成后，就要对数据漏洞进行分析，在技术方面，主要存在未修补的软件漏洞、弱密码、未加密的数据传输等漏洞。在管理方面，则是具有缺乏访问控制、未制定数据安全策略、员工安全意识不足等漏洞，这些漏洞会导致数据风险加大。

根据数据的风险和漏洞，管理人员就要利用计算机科学技术，对风险进行量化与评估，按照高、中、低等形式，来评估出威胁发生的可能性，同时也要评估数据风险对业务的影响程度。根据风险的评估结果，就可以制定出具体的风险缓解方法，例如，可以采用风险规避的方法，停止企业内导致数据风险的活动；采用风险转移的方法，通过保险或外包，来转移风险；采用风险缓解的方法，利用加密数据、部署防火墙等操作，来降低数据风险，让数据的使用更安全。通过对数据风险评估进行强化，就可以全面识别数据安全风险，并针对性提出管理措施，进而降低数据安全风险，保障了数据资产的安全性[3]。

2.3 开展数据风险预警

在开展数据风险评估后，就要实现风险预警管理，主要是通过计算机科学技术，提前识别和响应数据中潜在的安全威胁，以降低风险对数据使用产生的影响。在进行风险预警的时候，需要对数据资产、数据危险进行识别，并且要建立预警指标体系。对于技术指标则是多次失败登录、异地登录等行为；突发性流量增加等异常性行为；CPU、内存使用率突然升高等行为。对于业务指标则是数据篡改、丢失等完整性异常；服务中断、访问延迟等可用性异常；数据合规性异常等。一旦在监测的时候，发现了这些异常指标，那么就要及时进行预警，保证数据管理人员开展有效的防护措施。

在进行监测的时候，管理人员需要部署入侵检测系统和入侵防御系统，同时使用安全信息与事件管理工具，来集中监控数据使用日志。并使用 Nagios、Zabbix 等系统监控设备，来监控服务器的性能，使数据访问和操作都在监控下开展。然后就要设置预警阈值，对于技术指标的阈值是，登录失败次数每分钟超过 5 次、数据流量增加了 50%、CPU 使用率>90%等，就属于异常现象。对于业务指标的阈值则是，数据丢失或篡改超过 1%、服务中断时间超过 5 分钟、数据访问延迟超过 500ms 等情况，那么就要及时进行报警，让数据管理人员对其进行处理。当预警系统监控到指标已经超过了阈值时，就会自动触发预警，并通过邮件、短信、系统通知等方式，向数据管理人员发送预警信息，预警级别则根据风险等级设置低、中、高等不同的级别。管理人员就要根据预警级别来及时进行响应和修复，隔离异常的数据，防止数据风险产生扩散，同时也要修复数据漏洞，恢复数据正常使用。

2.4 实现数据备份管理

在数据管理中，运用计算机科学技术，可以高效的实现数据备份管理，保证数据使用的安全。通过数据备

份，能够防止数据出现丢失、损坏或篡改等情况，使数据能够在故障后，快速恢复。在进行备份的时候，可以采用全量备份、增量备份以及差异备份等方法，其中全量备份就是要备份所有数据，主要是在数据首次备份或定期备份的时候使用[4]。增量备份则是要仅备份自上次备份以来所产生变化的数据，这样的备份可以节省存储空间。差异备份则是要备份自上次全量备份以来产生变化的数据，使其恢复速度较快。备份数据每月开展一次，每次数据保留的时间为 90 天，保证数据备份更高效。同时，在进行备份时，可以采用本地备份的方法，使用硬盘、磁带等一些本地存储设备对数据进行备份，此技术的备份速度快，成本也比较低。也可以采用远程备份的方法，能够将数据备份到远程服务器或者是云存储当中，保证了数据的安全，使其不会受到本地灾害的影响。

在人员开展备份管理的时候，主要是使用了 Veeam、Acronis、Backup Exec 等备份软件，实现自动化备份效果，可以每天凌晨 2 点来执行增量备份技术。管理人员也要定期检查备份数据自身的完整性和可用性，并使用恢复测试，保证备份数据可正常恢复。在对数据进行备份储存管理的时候，就要把备份数据储存在硬盘、磁带、光盘或云存储当中，同时要根据数据的增长趋势，预留出足够的存储空间，并定期清理已经过期的备份数据，进而释放存储空间，减少数据对系统的影响。

2.5 增强数据访问控制

在开展数据访问控制时，主要是为了能够防止一些未经授权的用户，来访问敏感数据，保证数据的使用更安全。在访问控制中，一是基于角色的访问控制模型，这一模型主要是定义了管理员、编辑、查看者等不同的角色，并为每个角色分配权限，将用户分配到相应的角色当中，进而简化了权限管理。二是基于属性的访问控制模型，主要是根据用户所在的部门、职位等属性，动态控制访问权限。三是强制访问控制模型，根据数据自身的安全级别和用户的权限等级，来强制的控制访问。四是自主访问控制模型，允许数据的所有者，决定谁可以访问其数据。根据数据管理的实际情况，可以选择不同的控制模型来进行数据访问控制，进而保证数据控制效率得到提升。接下来，就要采用身份验证的方法，主要是结合密码、短信验证码等方式，来验证用户的身份，并根据身份权限来进行数据访问。在进行验证的时候，可以结合使用指纹、虹膜或面部识别技术，进而增强了身份验证的安全性。在进行授权管理的时候，管理人员要根据用户的角色或属性，为其分配数据的读、写、执行等权限，并在文件系统或数据库中设置权限继承规则，简化数据管理的流程，使得数据访问得到有效控制。

3 结论

综上所述，对数据管理运用计算机科学技术的方法进行优化分析，不仅提升了数据管理的效率，还使得数据共享更加便捷，行业连接更加紧密，促进社会经济稳定发展。运用计算机科学技术进行数据管理时，主要是从数据加密、风险评估、风险预警、备份、访问控制等方面入手，保证数据管理更加精准、高效，提升了数据使用的安全性。

参考文献

[1]钟幸.浅谈计算机科学技术在数据管理中的运用[J].中国设备工程,2024,(22):50-52.
[2]张振寰.计算机科学技术在数据管理中的应用[J].数字技术与应用,2022,40(06):124-126.
[3]陈幸真,刘萍.计算机科学技术在数据管理中的应用[J].数字技术与应用,2022,40(01):44-46.
[4]傅蕾,邹瑜.计算机科学技术在数据管理中的应用——以大学生心理健康教育网络平台为例[J].中国新通信,2022,24(02):109-110.

作者简介：王晨盛（2004.03-），男，汉族，福建泉州人，本科在读，研究方向:计算机科学与技术、面向对象的程序设计。