网络安全视角的数据安全保障技术

高菲
亚信科技（成都）有限公司　北京市　100000

【摘　要】步入数字化时代，数据已然成为企业与社会的关键资产。然而，网络安全威胁的持续加剧，给数据安全带来了极大挑战。本文从网络安全的视角出发，深入探究数据安全面临的多种威胁，系统阐述数据加密、访问控制、数据备份与恢复等数据安全保障技术的原理、适用场景及实践要点，并结合实际案例验证这些技术的成效，旨在为网络安全和数据安全领域的从业者提供参考，助力提升数据安全防护水平，推动网络安全行业的良性发展。

【关键词】网络安全；数据安全；数据加密；访问控制；数据备份

Data security technology from the perspective of network security

Gao Fei
AsiaInfo Technology（Chengdu）Co.，LTD. Beijing　100000

【Abstract】Entering the digital age，data has become a critical asset for both enterprises and society. However，the continuous intensification of cybersecurity threats poses significant challenges to data security. This paper，from the perspective of cybersecurity，delves into various threats faced by data security. It systematically explains the principles，applicable scenarios，and practical points of data security technologies such as data encryption，access control，and data backup and recovery. By combining real-world case studies to verify the effectiveness of these technologies，this paper aims to provide a reference for professionals in the fields of cybersecurity and data security，helping to enhance data security protection levels and promote the healthy development of the cybersecurity industry.

【Key words】network security；data security；data encryption；access control；data backup

一、引言

在信息技术高速发展的当下，数据的价值愈发突出，广泛应用于金融、医疗、教育等多个重要领域。但随着数据规模的爆发式增长，网络环境变得愈发复杂，数据安全问题频频发生。数据泄露、篡改与丢失等问题，不仅会给企业和个人造成严重的经济损失，还可能引发一系列社会问题。据相关权威统计，全球每年因数据安全事件造成的经济损失高达数百亿美元。在金融领域，客户账户信息一旦泄露，资金被盗取的风险将大幅增加；在医疗行业，患者病历数据若被篡改，会对患者的生命健康构成直接威胁。因此，在复杂的网络安全环境下，如何切实保障数据安全，已成为网络安全领域亟需解决的重要问题。

二、数据安全面临的威胁

2.1 网络攻击

网络攻击对数据安全构成了严重威胁。黑客凭借对网络漏洞的深入了解，如操作系统漏洞、应用程序漏洞等，入侵企业网络，窃取、篡改或破坏数据。常见的网络攻击手段丰富多样，SQL 注入攻击通过在应用程序输入字段中植入恶意 SQL 语句，获取或篡改数据库中的数据。例如，黑客利用某在线商城的 SQL 注入漏洞，获取了大量用户订单详情，包括商品选购记录、收货地址等。DDoS 攻击借助大量傀儡机向目标服务器发起海量请求，致使服务器因负载过高而瘫痪。曾有一家热门直播平台遭受 DDoS 攻击，直播服务长时间中断，观众无法正常观看直播，平台营收遭受重创。跨站脚本攻击（XSS）通过在网页中注入恶意脚本，窃取用户的敏感信息，如登录账号和密码。

以 2017 年肆虐全球的 WannaCry 勒索病毒为例，该病毒利用 Windows 操作系统的 SMB 漏洞，迅速传播，大量计算机被感染，用户数据被加密，黑客借此索要赎金，给无数企业和个人带来了巨大损失。此外，新型网络攻击手段不断涌现，如人工智能驱动的攻击方式，利用机器学习算法精准识别网络漏洞，加大了数据安全防护的难度。一些黑客借助深度学习技术，分析网络流量特征，绕过传统的入侵检测系统，对企业网络发动攻击。

2.2 内部人员违规操作

内部人员因拥有企业网络和数据的访问权限，其违规操作极易引发数据安全事故。部分内部人员受利益驱使，将企

业敏感数据泄露给竞争对手；还有些人因操作失误，误删或篡改重要数据。相关调查表明，约 30% 的数据安全事件源于内部人员的违规行为。例如，某企业员工为谋取私利，私自将公司客户信息出售给第三方，导致公司客户大量流失，声誉严重受损。

此外，企业内部员工的安全意识参差不齐，部分员工对数据安全的重要性认识不足，随意使用弱密码、在不安全的网络环境中处理工作数据，为数据安全埋下隐患。一些员工为方便记忆，使用生日、电话号码等简单数字作为密码，账号极易被破解。在公共无线网络环境下，部分员工处理企业敏感数据，黑客通过网络嗅探技术，轻易获取这些数据。

2.3 物理安全风险

物理安全风险是数据安全的重大隐患。数据存储设备，如硬盘、服务器等，容易受到自然灾害、火灾、盗窃等意外事件的影响，导致设备损坏或丢失，进而造成数据丢失。设备老化、长期高负荷运行导致内部零部件磨损，或出现硬件故障，如硬盘坏道、服务器主板短路等，也会对数据的完整性和可用性造成影响。

以某大型数据中心为例，该数据中心位于地震多发区，却未做好充分的防震措施。在一次地震中，大量服务器受损，存储在其中的重要数据无法恢复，依赖这些数据的企业业务陷入停滞，经济损失惨重。此外，数据中心的电力供应故障也会引发连锁反应。一旦停电，备用电源若无法及时启动或供电时长不足，服务器将被迫停机，正在进行的业务中断，数据处理流程被打断，可能导致数据丢失或不完整。温度和湿度控制不当同样会威胁数据安全。若数据中心温度过高，服务器散热系统无法正常工作，芯片过热可能导致服务器死机，数据无法正常读取；湿度过高则可能引发设备内部电路短路，腐蚀金属部件，降低设备使用寿命。

三、数据安全保障技术

3.1 数据加密技术

3.1.1 对称加密

对称加密是一种基础且常用的加密方式，加密和解密使用同一密钥。常见的对称加密算法有 DES、3DES 和 AES。DES 曾是行业标准，如今其安全性有所下降，但在某些特定场景仍有应用；3DES 通过多次应用 DES 算法，提升了加密强度；AES 凭借高效性和安全性，成为当前主流的对称加密算法。对称加密在处理海量数据时速度较快，适合大规模数据的加密存储和传输。但对称加密的密钥管理较为复杂，同一密钥既用于加密又用于解密，一旦密钥泄露，数据很容易被破解。企业可采用密钥轮换策略提升安全性，比如每季度更换一次加密密钥，降低因密钥泄露导致的数据风险。

3.1.2 非对称加密

非对称加密使用一对密钥，公钥用于加密，私钥用于解密。常见的非对称加密算法包括 RSA 和 ECC。RSA 基于数论中的因式分解难题，早期应用广泛；ECC 利用椭圆曲线离散对数问题，具有密钥更短、运算效率更高的优势，受到越来越多的关注。非对称加密在密钥管理方面具有优势，适用于复杂的网络环境，但加密和解密速度相对较慢。在数字签名和身份认证场景中，非对称加密发挥着重要作用。在数字签名过程中，发送方使用私钥对数据进行签名，接收方使用发送方的公钥进行验证，以此确保数据的完整性和真实性。在网上银行系统中，用户通过数字证书（包含公钥及身份信息）进行身份认证，银行通过验证证书来确认用户身份，保障交易安全。

3.2 访问控制技术

3.2.1 自主访问控制

自主访问控制（DAC）以用户身份为核心，构建了一种灵活的访问控制机制。在这种模型下，每个用户都有一个专属的访问控制列表（ACL），详细记录了该用户对不同资源的访问权限。以企业文件管理系统为例，文件所有者可根据实际需求，自主设置其他用户对文件的读、写、执行等权限。这种灵活性使得文件共享和协作更加便捷，但 DAC 模型也存在一定的安全隐患。由于用户自主操作权限较大，一旦用户因疏忽出现误操作，或遭受恶意攻击被利用，就可能导致权限分配不合理。比如，文件所有者误将敏感文件的写入权限授予无关人员，该人员就可能对文件进行恶意篡改，威胁数据安全。

3.2.2 强制访问控制

强制访问控制（MAC）基于安全标签体系，构建了严格的访问控制机制。在该模型中，系统为用户和资源分别赋予不同的安全标签，这些标签反映了用户和资源的安全级别。只有当用户的安全级别高于或等于资源的安全级别时，用户才能访问相应资源。MAC 模型在对安全性要求极高的领域，如军事、政府等，应用广泛。在军事指挥系统中，不同级别的军官根据其职责和安全等级，只能访问相应级别的军事信息，从源头上避免了因权限混乱导致的信息泄露风险。不过，MAC 模型在保障高安全性的同时，灵活性相对较低，在实际应用中，需要投入大量精力制定严格的安全策略并进行精细管理，以兼顾安全需求和工作效率。

3.3 数据备份与恢复技术

3.3.1 全量备份

全量备份旨在对所有数据进行完整备份。其最大优势在

于数据恢复过程简单直接，一旦数据丢失或损坏，可直接从备份文件中进行完整还原。但全量备份所需时间较长，且占用大量存储空间。考虑到企业数据量的持续增长，为平衡数据完整性和备份效率，企业通常制定定期全量备份计划，如每月执行一次。为提高全量备份效率，可采用并行备份技术，利用多个备份设备同时进行数据备份。例如，大型企业的数据中心通常配备多台备份服务器，通过合理配置，这些服务器可同时对不同数据分区进行全量备份，大幅缩短备份时间，减少对业务系统正常运行的影响。

3.3.2 增量备份

增量备份仅对自上次备份以来发生变化的数据进行备份。这种方式显著减少了备份所需时间和存储空间，尤其适用于数据变化频繁的场景。但在数据恢复时，由于每次增量备份仅记录部分变化数据，需要依次还原多个备份文件，过程相对复杂。为优化数据恢复流程，企业可在全量备份的基础上，每天进行增量备份，在提高备份效率的同时，降低数据恢复难度。此外，引入差异备份作为补充手段，差异备份仅记录自上次全量备份以来所有变化的数据。这样，在数据恢复时，只需还原全量备份文件和最近一次的差异备份文件，即可快速恢复数据，大大简化了数据恢复流程，提高了数据恢复效率，保障企业在面对数据危机时能够迅速响应。

四、案例分析

4.1 案例概况

某金融机构在数据安全防护方面面临严峻挑战。由于业务的特殊性，该机构存储了大量客户的敏感信息，如身份证号、银行卡号、交易记录等。一旦这些数据泄露，将给客户和机构带来巨大损失。为保障数据安全，该机构采用了一系列先进的数据安全保障技术。

4.2 实施措施

在数据加密方面，该机构对客户敏感信息采用 AES 对称加密算法进行加密存储，并使用 RSA 非对称加密算法对对称密钥进行加密传输，确保数据在存储和传输过程中的安全性。在访问控制方面，采用基于角色的访问控制（RBAC）模型，根据员工的职责和权限分配不同的角色，每个角色拥有相应的访问权限。例如，客服人员只能查看客户的基本信息，而财务人员可访问客户的交易记录。在数据备份与恢复方面，每月进行一次全量备份，每天进行增量备份，并将备份数据存储在异地服务器上，以防止本地数据中心发生灾难时数据丢失。此外，该机构还定期对员工进行数据安全培训，提高员工的数据安全意识。

4.3 实施效果

通过实施上述数据安全保障技术，该金融机构的数据安全防护水平得到显著提升。在面对多次网络攻击时，成功抵御了黑客的入侵，未发生数据泄露事件。在数据恢复方面，当服务器出现故障时，能够快速恢复数据，保障了业务的正常运行。在一次服务器硬件故障中，通过异地备份数据，该机构在短时间内恢复了业务系统，将损失降到最低。此外，通过员工培训，员工的数据安全意识明显提高，因内部人员违规操作导致的数据安全风险大幅降低。

五、结论

在数字化时代，数据已成为企业和组织的核心资产，数据安全是网络安全的重要组成部分，其重要性不言而喻。随着信息技术的快速发展，网络攻击手段不断更新，从常见的恶意软件、网络钓鱼到高级的零日漏洞攻击，威胁形势日益严峻。在这种背景下，企业和组织应综合运用多种数据安全保障技术。通过数据加密技术，对敏感数据进行加密处理，保障数据在传输和存储过程中的保密性；实施精细的访问控制机制，根据用户角色、权限和数据敏感度，严格限制数据访问，防止非法越权访问；建立完善的数据备份与恢复策略，定期备份重要数据，确保在数据遭遇丢失、损坏或攻击时，能够快速、准确地恢复数据，保障业务的连续性。此外，加强对内部人员的管理和培训至关重要，定期组织数据安全培训，向员工普及数据安全知识、常见风险及应对措施，提高全体人员的数据安全意识，从源头上减少因内部人员疏忽、违规操作等引发的数据安全事故。展望未来，随着量子计算、人工智能等新兴技术的不断发展，数据安全保障技术也将持续创新和完善，为网络安全和数据安全提供更强大的保障，助力企业和组织在数字化浪潮中稳步前行。

参考文献

[1]吴世忠，等。信息安全原理与技术 [M]. 北京：清华大学出版社，2019.
[2]陈钟，等。网络安全 [M]. 北京：人民邮电出版社，2018.
[3]段云所。数据安全原理与实践 [M]. 北京：机械工业出版社，2020.