大数据环境下的数据安全分析与探讨

牛曦恺
杭州合众数据技术有限公司　浙江　杭州　310000

摘　要：大数据的基本特征表现为数据规模庞大、数据类型复杂。目前，大数据的技术手段已经充分渗透至各行各业。网络数据信息安全将直接关系到网络用户的人身安全和财产保护，因此关键是要充分利用数据安全监管和保护措施，全方位防范网络数据信息潜在的安全风险因素。本文对大数据环境下的数据安全进行了深入的分析。

关键词：大数据；数据安全；分析

引言

数据安全风险对人民群众的正常生活和行业生产发展有不可忽视的效果。如果不能及时发现和控制数据安全风险，网络数据信息的传输和共享将遇到重大阻碍。在当前大数据时代的技术变革背景下，数据安全风险的共同表现呈现出多种多样的整体发展特征，网络用户的隐私和安全利益可能受到威胁和损害。可见，要全方位防范和监测数据安全风险，科学合理选用大数据信息处理和共享平台。

1 大数据环境对数据安全有重要影响

大数据的本质在于对规模庞大、类型复杂的网络数据资源进行整合。大量数据信息的融合过程呈现出动态的整体发展特征。因此，需要采取使用专门的数据分析和集成技术方法，进行必须的归纳处理。在当前网络数据信息传播实践中，大数据最关键的表现形式是其规模大、增长速度快、种类繁多、信息价值密度低。大数据的专业处理与分析技术已充分融入社会生产发展的各个实际领域，重点关注教育、医疗等公益领域、企事业单位的经营管理过程、动态传输过程的网络数据信息。

大数据环境能够准确感知数据信息的动态变化过程，但同时也提高了数据信息泄露和丢失的潜在风险。大数据专用处理工具平台可容纳庞大海量的网络数据资源，未妥善保护的网络数据资源将相对容易遭到破坏和窃取，从而提高网络用户的明显利益损失。由此能够判断，综合防控、准确预测数据安全风险因素具备重要的信息安全价值。

2 大数据环境下的数据安全风险

2.1 用户隐私泄露风险

用户隐私信息的范围具备多样化的特点。如果用户隐私信息得不到适当的监管和保护，未经必要保护的用户隐私数据就会暴露在网络黑客等不法分子的眼中。当前形势下，泄露用户隐私数据信息的方式多种多样。如果企事业单位的运营技术人员和个人网络用户没有设置网络防火墙等必须的安全监管措施，将进一步提高用户隐私信息的泄露。可能性。不法分子将出售或借助窃取的用户隐私数据谋取非法经济利益，严重阻碍了整个社会正常运行秩序的实现。

2.2 网络攻击的表现形式多种多样

大数据平台客观上提高了网络安全攻击的具体表现形式，从而致使现有网络安全攻击形式向隐蔽性和多样化发展。在某些情况下，大数据信息传播平台本身也能够构成攻击网络、侵犯用户安全的重要工具。一种典型的网络攻击形式是设置隐藏的网络程序代码，并对恶意程序代码进行马赛克处理。攻击网络信息系统的犯罪分子更善于借助现有的网络安全漏洞，从而致使各种安全和隐私侵害事件频发。可见，多样化的网络安全攻击表现形式的存在，将明显威胁到整个网络的安全稳定运行，甚至造成网络系统的整体瘫痪。

2.3 数据安全管理基础设施存在缺陷

网络数据安全管理的实践不能缺少必须的基础设施支撑，但现有的数据安全管理基础平台存在多层次的安全漏洞，将难以做到集中的网络数据传播、数据采集和数据共享。这个过程带来干扰和破坏。具备分布式和虚拟化特征的大数据和云计算技术支撑平台很可能已然成为窃取和破坏用户隐私信息的工具。网络黑客在未经授权进入网络数据系统时，会频繁攻击整个网络设备，造成云存储大规模数据信息被盗。未定期检测、维护和更新的网络安全管理基础设备存在薄弱缺陷，提高了数据安全隐患。

3 大数据环境下确保数据安全的措施

3.1 不断增强人员信息安全意识

数据安全不仅是个人数据安全，更是企业和国家数据安全，维护数据安全十分重要。在进行维修时，人员的安全意识不可或缺。只有提升他们的意识，才能减少

随机数据流通的现象，明白如何保护我们的隐私。能够用视频和标语让人们了解数据安全的重要性，让人们学会辨别网络上的真实信息，不要随意在网络上传播重要的资料，也不要点二——互联网上的维度信息、代码和链接。只有增强人员的自我保护意识，才能降低数据被盗的风险，保障网络的安全。在企业中，要想保证数据安全，就一定要借助培训的方式，进一步增强员工的安全意识，定期对员工进行培养训练和宣传，让员工了解数据安全，并在培训结束后进行考核，确保员工的学习效率，进一步提升员工数据安全保护意识和能力，让企业数据在应用中更加安全。

3.2 增强数据安全管理

在管理数据安全的过程中，需要从不断增强管理制度、构建安全认证体系、监管数据三个方面进行。在增强数据管理体系的同时，政府需要增强数据安全方面的法律。一旦出现非法窃取数据的现象，一定要予以行政处罚或拘留。一定要严惩违规行为，在最本质的角度上来降低数据风险，确保数据信息在健康的网络环境中传播，构建安全认证体系。人员在查阅网络信息时，需要对个人身份信息进行身份验证和登录，以保证数据的合法使用。认证通过后，相关部门和技术人员还一定要核实数据参考情况，了解和调查，减少非法选用数据信息。需要对数据进行监管，确保网络上的数据实时完整、安全。加强监管执法工作，对部分非法窃取信息的案件，能够借助没收违法所得、关闭网页、吊销许可证等方式严厉查处，增强管理措施。

3.3 增强非法侵权防范技术

在互联网上，数据的传播和获取非常方便，但同时也很容易在传播过程中受到非法攻击。如果想到达这样的效果，必须保证数据的安全，减少资金和信息的损失，一定要增强安全防范技术，能够借助数据管理、评估、监控等措施来提升数据的安全性。在进行检测时，能够借助防火墙、入侵检测等技术检测数据的传输和存储情况，借助防火墙进行防御，保证终端与外网接口的保密和安全，从而保证数据安全更有效的抵抗网络入侵。同时，还需要监控内部网络情况，真正识别计算机中潜在的数据风险，检测系统中的漏洞和缺陷，然后选用杀毒软件清除入侵的病毒，使系统漏洞被消除。打补丁保证了整个计算机软件在应用过程中的安全，维护了网络的稳定。数据安全的根本在于保障网络安全，因此需要增强网络安全，在最本质的角度上来维护数据安全。为防止黑客窃取非法数据，在预防时能够采取使用访问限制技术来控制用户的网络访问，借助大数据技术构建访问认证和权限体系，借助身份认证和权限管理来进行访问更安全，确保人员在访问数据时得到证书和用户的授权，从而增强网络安全。另外，从国家的角度来说，需要支持安全保护技术，能够提供技术、资金、政策等方面的支持，为人员和企业予以数据保护，减少违法侵权行为的发生。

3.4 模式识别认证系统

模式识别认证系统由数据采集、数据转换和模型匹配三部分组成。它看起来很像手机中的指纹识别或眼睛虹膜识别功能。在模式识别系统的设计过程中，需要提取和选择应用的特征和相应的主题。计算机智能学习、样本选择测试等步骤，为了进一步提升模式识别认证的结果，一般需要加入人工规则，也能够限制各种条件，缩小搜索空间，达到缩短的目的把计算量降到最低。生物安全技术被认为是最安全可靠的模式识别方法，普遍作用于高度机密数据领域，但鉴于这种认证方式过于复杂，并不是所有的数据安全操作都能够在生物认证方式中进行。为了能够广泛选用这种高安全性技术，云计算服务能够借助应用信息认证和可信融合验证证明技术，帮助用户安全进入系统，帮助用户解决无法选用生物认证的问题，是一种高安全性的方法。用户在注册云计算服务时能够设置密码锁和密码密钥，在选用过程中能够输入密码密钥被认为是进入云计算环境的必要条件。甚至用户能够借助短信验证码、回答指定问题、协助他人、绘制既定图形等多种模式验证方式来开启密码锁。该方法的应用能够保证在安全的前提下向用户予以云计算服务。

3.5 完善数据安全管理基础体系

为解决和应对大数据发展趋势带来的数据安全风险，应尽快完善监管部门现有的数据安全管理基础平台。尽快构建数据安全管理网络体系，确保数据安全管理基础体系得以集成多层次的安全检测和控制功能。例如，对于大数据和云计算的数据安全监管模式，关键是做到数据资源共享、网络信息一体化处理、网络安全自动监测、预防和保障机制。近年来，人工智能和数据挖掘与处理等技术手段全方位投入实际应用领域，客观上达到了完善数据安全管理基础设施、减少非法选用网络数据资源损失的效果。

3.6 提升数据安全防范能力，保障数据安全传输

完善的网络保护体系和有所关联的访问管理，能够有效保护数据信息的安全，使大数据云计算等整体系统得到一定程度的保护。从某种角度看来，对于用户的访问，应进行后台数据的查询，认真保存用户访问的痕迹，以达到

有效的数据传输和下载安全。科学选用防火墙技术，该技术的主要作用是防止部分黑客侵入公司或组织内部的信息系统和数据，从而抵御不法分子的攻击，为云下大数据分析的安全传播筑起一道高大的“抵抗墙”计算。为做好公司内部检测工作，积极挖掘大数据系统中的潜在威胁，构建科学有效的大数据信息安全防护体系，使大数据信息得以传播和传播，共享更安全。

3.7 实施审计和监督措施

为最大限度降低我国大数据云计算平台的安全风险，所有参加的平台提供商都需要通过上级部门的严格审核。审核内容包括但不限于其提交的软硬件产品，对其安全对抗机制及其内部管理制度进行全方位审查。借助这个环节，各予以商逐步形成有效的大数据风险对抗机制，确保其提交的业务安全。在预警条件下，所有应用程序将被系统锁定，不能用于高危用途，如更改账户密码、数据复制迁移等，连续3次身份错误，将无法选用，不再支持再次登录。应该在技术人员介入并仔细检查情况后，才能再次快速释放登录权限。

3.8 完善数据隔离体系，完善数据监控方案

对于活跃复杂的大数据云软件，不仅要包含构建完备的维护体系，还需要特别关注相关的管控管理方法和管理技术。一方面，为大数据云软件构建了强大的技术后盾，避免被他人随意攻击；另一方面对所选用的金融数据进行合理监控，确保客户在选用数据时得到合理维护。因此，技术要让金融数据在信息系统中更易于管理，就需要借助各种维度对金融数据进行更深入、更有层次的综合预处理，重点是保证数据的相对安全性；但是一旦客户想要选用原来的软件，就只能去数据中心加载解密了。如果想达到这样的效果，必须避免数据长期丢失甚至被清除，客户还能够选用存储卡、U盘、网盘等数据资料对其进行保护，为数据带来多重保护。或者直接采取物理隔离的方式，虽然数据稳定性越来越好，但是这种方式的数据分散度比较高，不方便数据管理。

3.9 善用信息数据加密软件，并做好相应的数据备份工作

用户数据的正常传输和共享，需要对文本、信息等内容进行保密，为数据填上“第二把锁”。同时，用户在传输金融数据时也需要注意，无论文件内容是否保密，未来仍将在用户内部做到正常传输和共享；如果用户想选用原始文件，能够直接在数据中心下载解密。如果想达到这样的效果，必须防止文件长期丢失或被清理，用户能够选用存储卡、U盘、网盘等存储物品进行保存，为文件予以多重保护。或者用户能够选用物理隔离。

结语

通过分析可以看出，大数据新的发展背景在促进网络数据信息资源共享的同时，也埋下了数据安全受损的潜在威胁。近年来，网络数据信息被盗用、被冒用的安全风险与日俱增，不法分子善于借助大数据网络信息监管机制的漏洞，侵害广大用户的合法权益。为应对和化解网络数据信息安全隐患，现阶段的关键应对路径应是健全数据安全预警设施体系，提升网络用户安全防护意识，构建完善的数据保护体系。

参考文献

[1]韦超英,苏珍,李海强.大数据环境下计算机网络信息安全的对策研究[J].信息记录材料,2022,23(06):75-77.

[2]韩文瑾.大数据云计算环境下的数据安全分析与对策分析[J].中国新通信,2021,23(22):134-135.

[3]乐文城.大数据环境下数据安全风险对策浅析[J].电子元器件与信息技术,2021,05(08):141-142.