

大数据应用中数据安全治理技术研究

刘 洋

咪咕音乐有限公司 四川成都 610000

摘要: 随着信息技术的不断发展,大数据应用范围不断扩大,成为社会经济发展的主要动力。大数据作为一种新的技术手段,在推动社会经济快速发展、提升企业核心竞争力等方面具有重要意义。然而,由于数据应用安全水平低、信息共享不畅等问题,数据安全问题已经成为制约大数据应用的主要瓶颈。文章从大数据应用的全生命周期出发,依据大数据应用中数据安全治理问题进行分析,探讨了信息安全治理措施,以期使广大大数据用户对现有的安全技术有更多的认识,从而转变新的安全思想。

关键词: 大数据; 数据安全治理; 技术研究

Research on data security governance technology in the application of big data

Yang Liu

Migu Music Co., LTD., Chengdu, Sichuan, 610000

Abstract: With the continuous development of information technology, the application scope of big data is constantly expanding, becoming the main driving force for social and economic development. As a new technological means, big data is of great significance in promoting rapid social and economic development, improving the core competitiveness of enterprises and other aspects. However, due to problems such as low data application security level and lack of information sharing, data security has become the main bottleneck restricting the application of big data. This article analyzes the issue of data security governance in big data applications based on the full lifecycle of big data applications, and explores information security governance measures, in order to enable the majority of big data users to have a better understanding of the existing security technologies and thereby transform their new security concepts.

Keywords: big data; data security governance; technology research

引言

随着网络信息技术的不断发展,大数据成为社会发展的主要动力。大数据是指在某一时间内数量巨大、类型多样、具有多种属性和多个来源的数据集合,它为经济、科学等领域提供了大量有价值的信息和服务。当前,我国大数据产业呈现蓬勃发展态势,大数据应用范围不断扩大,已经成为促进社会经济加快发展的主要动力。然而,随着大数据应用范围越来越广,其安全风险也越来越高。数据泄露、网络攻击、隐私泄露等现象层出不穷,严重影响了人们使用大数据技术的热情与积极性。因此,为进一步促进社会经济稳定发展,保证企业数据安全至关重要。

一、大数据技术

在传统的数据库中,数据往是以文本的形式存储的,并不能够实时地处理数据,无法有效地分析和利用用户所产生的信息。随着计算机技术和通信技术发展,大数据技术应运而生。通过对海量实时信息进行处理和分析,从而达到对社会经济快速发展有重要意义的领域或者行

业中产生或积累大量信息,对大数据进行分析和处理后,可以发现其中所蕴含的价值。大数据作为一种新的网络概念和应用模式,在社会经济快速发展下逐渐成为企业竞争战略中至关重要的一部分。

二、数据生命周期

数据生命周期可以从某种意义上反映出不同的数据发展过程和发展规律,而数据生命周期也因其目标而异,比如云数据生命周期。数据的生命周期一般以全过程监视为基础,将后续的数据传输过程分为准备、储存、使用和销毁等多个阶段。

数据的准备阶段是数据利用的一个重要前提,它包括数据的生成、筛选和收集,它能很好的处理数据资源的分布,同时也能满足不同的数据利用需求。数据的生成的实质是新数据的产生,不管是基于软件服务产生的原始数据,还是根据已有的数据产生新数据,都可以作为数据产生处理。在进行数据筛选时,最重要的是数据的可用性。没有经过筛选的数据都是无效的,需要进行进一步的处理。数据收集就是改变数据储存地点,比如

个体使用者利用计算机的上载数据至云端。

在数据的使用阶段，数据分析、数据规模计算、数据协同，是实现数据应用价值的关键时期。数据分析的目标是理解和发掘数据的价值，运用自动化的分析方法，利用大数据模型进行分析；大规模的数据运算，是指运用数据分析的结果。数据合作就是利用各种主体来完成不同数据作业（如图 1 所示）。



图 1 数据分析

在数据储存阶段，必须把数据储存在一个特殊的储存空间内，并且要随时进行调用准备。在这段时间内，为了防止数据泄露，必须加强数据的安全性。

在数据销毁阶段，数据可以在任何时候被销毁，而被销毁的数据无法再利用。使用者必须发出销毁证明，如果拥有者想要使用被销毁的数据。

三、大数据信息安全治理存在的问题

3.1. 信息安全重视度不高

随着大数据技术的不断发展，大数据信息安全治理也逐渐成为信息系统建设与维护过程中的一项重要内容。在当前数据应用过程中，对数据安全问题的重视程度不够，导致出现了大量敏感数据泄露和非法访问等现象，严重影响了大数据资源整合应用能力的提升。由于大数据技术发展还不成熟，加上企业相关工作人员的专业知识水平有限，在处理大数据应用过程中出现的问题和风险不能及时发现和应对。目前我国大数据应用技术已经达到一定水平，但是由于企业内部系统、信息系统等众多复杂结构影响，加上信息处理技术落后，导致当前大数据管理和运行存在很大问题。另外，由于企业内部工作人员对于大数据的了解程度不够，导致企业存在着很多漏洞，这些漏洞为不法分子提供了可乘之机。由此可见，大数据信息安全治理在企业实际建设中是一项艰巨而又复杂的工作，企业需要建立完善的大数据信息安全治理体系来确保大数据环境下各项工作有序进行。

3.2. 敏感信息保护技术不足

虽然我国的敏感信息保护技术在大数据应用中取得了长足的进步，但仍存在不足之处。例如：如何防止在传输过程中出现泄露和篡改？如何防止存储在设备上的敏感信息被黑客获取？如何防止个人身份信息被窃取而导致的泄密呢？如何防止敏感数据向第三方开放？或者说如何实现敏感数据跨区域存储以避免泄漏呢？这些问

题需要在大数据技术应用过程中解决。但是，大数据平台对这些问题的解决能力仍然存在较大的局限性，目前仍无法从根本上解决问题。这也是目前数据安全治理工作难以取得突破重要原因之一。

3.3. 大数据库建设及维护水平低

大数据应用是一个庞大的系统工程，涉及多个领域、多个环节，涉及到诸多领域。从基础架构上看数据库管理系统是数据的载体，其技术与架构的优劣直接影响数据存储与处理能力。在大数据时代下，如何实现大数据系统及数据库的智能化，实现数据间快速有效匹配与共享是重中之重。虽然大数据库有诸多优势，但是目前我国大部分大数据库都存在着一些问题。

3.4. 数据安全性评价与预警机制不健全

当前，在大数据的背景下，数据安全技术保障体系尚未建立健全。一方面，大数据应用场景的不断丰富，对数据安全性评价与预警技术提出了更高、更深入的要求；另一方面，大数据领域中数据量大、类型多样的特点也使得传统安全保障技术难以满足大数据应用环境下的数据安全防护需求。此外，目前大部分企业、高校等对企业组织机构在组织架构建设方面较为单一。企业与高校在人才培养方面也缺乏合作，未能充分发挥各自优势；其次，高校自身对于网络环境下海量数据的处理能力不足，尚未建立起具有代表性和针对性的大数据应用平台。同时，大数据时代带来了许多新的挑战：大数据技术对个人隐私保护提出了更高要求；政府对企业进行监管需要进一步加强；国家间竞争也将不断加剧等等。这些新情况新问题迫切要求我们要高度重视大数据环境下的信息安全问题与挑战，大数据产业在促进经济社会发展过程中扮演着重要角色。

四、大数据信息安全治理技术措施

4.1. 提高信息安全的重视度

大数据时代，信息安全问题更加凸显。信息安全问题不仅涉及国家、企业和个人，更与整个社会的方方面面紧密相关。从国家层面上来说，信息安全关乎国家、企业、公民的切身利益与国家和社会的长远发展。而从社会层面上来说，信息安全关系到全社会的生存和发展。因此，我们需要从社会层面上提高对信息安全重要性的认识，采取积极有效措施提高信息安全。在新形势下，数据是重要的战略资源以及经济发展新动力。在大数据时代来临之际，对数据进行科学有效的处理将会产生很大用处，大数据不仅能提升企业生产效率、降低运营成本，而且还可以实现资源有效配置。从个人层面上来说，每个人都会有自己的数据资源空间以及信息空间。这些空间的存在让我们拥有了一份宝贵而无形的资产。如果个人想要进行数据交易或进行大数据分析时，必须要对数据具有相当程度上的控制和使用价值。

4.2. 建立相关的法律法规

首先，数据安全法律法规的制定是必要的。在数据

安全治理过程中,既要考虑到大数据应用的特点,也要考虑到我国目前国情的特殊性,以国家层面为主导。大数据信息安全法律法规应该与大数据技术发展相适应。在大数据技术发展过程中,法律法规需要做出相应的调整,避免出现与实际不符的内容。其次,大数据应用过程中应当加强个人信息保护的工作。在个人信息保护过程中,数据信息提供者和处理者应该对自身数据进行一定的保护,不能将这些数据随意地被提供给其他用户使用。最后,大数据应用需要加强相关行业和组织的协调和监管工作。大数据技术在各个领域的深入运用是必然趋势,行业之间以及不同业务之间有可能出现互相竞争、共同发展的情况,对此需要加强协调和监管力度。

4.3. 威胁感知的数据收集和清洗

大数据时代,数据具有海量、多元、复杂、多变的特点,在收集数据时很难做到有效地去分类和识别。在这个过程中,数据安全治理就是为了保护大数据资产免受黑客攻击而产生的。对海量数据进行高效准确地清洗处理,可以有效地降低数据风险,提高数据信息的准确性和有效性。大数据时代的大数据安全治理技术框架由两个方面组成:一是对大数据进行有效地收集、分类和清洗;二是从大数据存储到应用过程中对大数据的访问策略制定及行为监控。因此首先要完成对采集到的网络威胁信息进行有效分析处理,然后根据分析结果制定出符合实际情况的大数据采集方案和安全管理机制。

4.4. 数据安全治理技术框架

大数据应用中,需要将数据安全治理工作贯穿其中。为了提高数据应用的安全性和可靠性,需要在数据共享和使用的过程中采取相应的技术措施与手段。当前对大数据安全风险评估技术包括多维风险评估和数据安全审

计,多维风险评估是指通过对收集到的海量数据进行综合分析而得出相应结论,是对数据安全性与可靠性指标综合评价。目前对于大数据安全风险评估技术已经有了比较成熟的技术手段。主要包括数据挖掘和机器学习技术、信息安全审计等,通过收集相关数据信息,建立数据库日志、相关分析指标等作为评估依据,得出相应结论并提出应对策略。本文基于大数据安全风险评估以及数据审计方面的经验,构建了具有一定通用性和可扩展性的大数据安全治理技术框架。

五、结束语

综上所述,随着信息化建设不断推进,企业应用大数据技术已经成为必然趋势,然而,由于大数据的重要性,其在建设过程中存在一定的风险和隐患。因此,要想保证大数据应用的安全性和稳定性,必须从源头上对大数据安全治理进行管理。在当前阶段我国已经出台了相关的法律法规和行业标准,然而在实际应用过程中还存在一定的不足之处。因此在今后的工作中需要进一步完善大数据安全治理体系,从根本上提升大数据安全性和稳定性。

参考文献:

- [1] 荆舒煊,杨浩.新形势下数据安全治理体系研究[J].现代信息科技,2022,6(07):137-140+143.
- [2] 高磊,赵章界,宋劲松,翟志佳,杨芬,蒋宋.大数据应用中的数据安全治理技术与实践[J].信息安全研究,2022,8(04):326-332.
- [3] 倪舒婷.大数据时代政府数据安全治理能力研究[D].北京化工大学,2021.
- [4] 张涛.大数据视域下的国家安全治理理论析[D].郑州大学,2020.