

大数据时代数据分析与信息安全防护

陈志涛 富译萱 郭铭雅 李苗苗 陈于雅

顺德职业技术学院智能制造学院

DOI:10.12238/jpm.v3i5.4909

[摘要] 现阶段,科学技术的发展,促使整个社会迈入到大数据时代,而大数据技术也得到了广泛的应用,为数据分析提供了技术支持,保障了数据分析的准确性,与此同时,也带来不少信息安全问题,比如,信息泄露问题、病毒及黑客入侵风险等等。面对这种情况,相关单位应该对大数据时代特点予以了解,并对相关信息安全问题进行深入了解与全面掌握,明确信息安全问题产生的具体原因,针对具体原因,引进先进的安全防护措施,并制定出完善的应对方案,以此保障数据信息的安全性,以防其出现泄露风险,这样也有助于增强单位自身的信息防护能力,促进其自身的长远发展。

[关键词] 大数据时代; 数据分析; 信息安全防护

中图分类号: TN919 **文献标识码:** A

Data analysis and information security protection in the era of big data

Zhitao Chen Yixuan Fu Mingyan Guo Miaomiao Li Yuyachen

Shunde Vocational and Technical College College of Intelligent Manufacturing

[Abstract] at the present stage, the development of science and technology, prompted the whole society into the era of big data, and big data technology has been widely used, provides technical support for data analysis, ensure the accuracy of data analysis, at the same time, also bring a lot of information security problems, such as, information leakage, virus and hacker risk and so on. In the face of this situation, the relevant units should understand the characteristics of big data era, and further understanding and comprehensive grasp, clear information security problems, specific reasons for specific reasons, the introduction of advanced security measures, and develop a perfect response, to ensure the security of data information, in case of its leakage risk, it also helps to enhance the unit's own information protection ability, promote its own long-term development.

[Key words] the era of big data; data analysis; information security protection

引言

处在当下大数据社会时代中,相关企业单位在经营运行过程中,会产生大量的数据信息,而且形式多种多样,若是对其进行人工处理,则容易出现误差,并且会影响数据信息的应用效果。在这种情况下,相关单位就需要借助大数据技术对大量数据信息进行处理,这样则能够提高数据处理分析的精确性。不过,相关单位还应该注重数据信息的安全性,由于网络的开放性特点,导致信息系统中的数据信息容易受到网络病毒、黑客的入侵,因此,相关单位应该将信息安全防护工作落到实处,使其更好适应大数据时代的发展趋势。

1 大数据时代下的数据分析问题

1.1 抽样量化存在问题

在当前的大数据时代中,在对数据进行分析时,不需要将少量的数据作为样本,应该获取到全部数据信息,并对其予以分析。在以往的抽样分析中,样本的稳定性相对较低,随机性比

较强,而且在明确调研目标的情况下,还会在调查内容及界限等方面受到人为因素的影响、制约。在具体的实践调查工作中,侧重点的不同也会使得整体抽样数据的具体情况难以得到有效反映。另外,若是样本数据受到较大的限制,那么抽样结果的准确性也会受到一定的影响,这也会提高犯错几率,同时也会降低样本抽样的效率及质量^[1]。

1.2 数据计算较为模糊

处在当下的社会时代中,数据信息的数量越来越多,且具有较高的复杂性,与此同时,数据本身的准确度也正在不断下降。由于数据规模相对比较大,也因此,对追求数据准确度的可能性也比较低。在对数据进行测量计算时,会因为一些不可控因素或者是人为因素,致使数据本身的准确性有所降低。在大数据的时代背景下,数据信息非常多,且质量参差不齐,其中存在很多准确度不高的数据信息,所以,在对其进行计算分析时,需要对具有较高价值的数据予以准确把控。对于准确度

相对比较低的大数据而言,其本身也并非是有意识生成的,在这种情况下,若想获取到准确性较高的数据信息,则要提前做好相应的预防工作。

2 大数据时代下数据分析及信息安全防护风险

2.1 信息安全风险相对比较高

在大数据的时代下,数据信息呈现出爆炸式的增长状态,这些数据信息可以通过网络实现共享,也能够借助相应的云储存空间对相关数据信息进行储存,而且储存成本也比较低,这就导致数据信息的产生数量变得更多,从而提高了数据分析的难度。由于大量数据信息的涌入,使得人们接收的数据信息缺乏一定的准确性,所以,在面对大规模的数据信息时,应该做到有效提取。在具体的数据处理中,应该明确大众的实际信息需求,并将其作为相应的价值导向,在这一导向的引导下,落实数据分析工作,帮助大众对有关事物的信息予以准确了解,再将其传递给大众,进一步提高数据信息的准确性。在这一过程中,信息安全风险也会有所增加,并且会对网络用户造成一定的影响。比如,相关用户在网浏览一些商品时,在浏览信息就会被储存在大数据之中,有关商品营销企业则会根据这些信息,为用户推荐相似的商品信息,不过,由于用户浏览信息被采集以及储存,会导致其个人信息出现泄露风险^[2]。

2.2 少数企业恶性竞争,无法保障个人隐私安全

在大数据时代下,各种数据信息非常繁杂,其中就涉及到个人的隐私信息,个别企业在市场竞争中,为了获取更大的优势,会将个人隐私信息当作“商品”,并对其进行售卖或者是共享,这就对个人信息造成较大的威胁。比如,手机中的一些APP,可能会在用户不知情的情况下,在其使用软件的过程中,获取其应用位置、应用时间以及信息记录等等,而且会将收集到的信息传输到相应的服务器之中,导致用户个人隐私被公开,致使个人隐私受到严重的侵害。

2.3 信息安全防护力度较低

大量的数据错综复杂,其中包括结构化、非结构化的数据类型,其中非结构化的数据信息基数比较大,其自身的价值也不高,所以,很多企业在进行数据信息的收集、储存以及分析时,很容易忽视这类数据信息的安全防护,致使非结构化的数据信息存在安全风险。另外,部分企业对于数据信息的安全防护缺乏较高的重视,也因此,其对数据信息的安全防护力度较低,防护水平始终停滞不前,甚至出现信息泄露的情况,不仅会危害到数据信息的安全性,还会对企业自身的发展造成不良影响^[3]。

3 大数据时代下数据分析、信息安全防护的有效措施

3.1 提高数据分析以及存储水平

相关企业若想保障数据信息的安全性,则需要采用合适的方法,提高数据分析水平,同时也要对数据储存技术及逆行科学优化,从这两个方面,加大对数据信息的保护力度,进一步提高信息的安全性。

其一,提高数据分析水平。相关企业在强化数据分析能力时,

需要对信息涌入口予以全面控制,以防大量数据信息在同一时间内全部涌入进来,否则就会加大数据信息的分析难度。通过对数据信息涌入量的合理控制,能够在一定程度上降低数据信息的分析处理难度,确保分析处理工作的质量。现阶段,相关企业可以充分利用大数据技术,对大量的数据信息进行科学分析以及处理,同时也能够在第一时间发现数据信息内部的潜在安全隐患,这样也能够对其进行及时处理,进而降低数据信息的安全风险。比如,相关企业在借助丰富的信息及先进的大数据技术,对认证系统技术进行开发,或者是构建数据分析系统时,可以提前将一些恶意信息、没有任何价值的信息全部排出在外,以此减少其中的安全隐患,保障数据信息的安全性,避免信息系统存在漏洞,影响数据分析准确性。另外,在对数据信息的流量进行控制时,需要根据大数据云储存容量、数据分析水等,对信息涌摄入量予以明确,设置合适的控制目标,实现对数据信息涌入量的科学控制,借此保证涌入储存空间的数据信息的稳定性,这就避免了因信息过度涌入,产生无法处理的问题。与此同时,相关企业在对数据进行分析时,需要完善数据处理标准体系,设置相应的处理标准要求,使得涌入的数据信息的价值得到保障^[4]。

其二,有效扩充数据储存容量。相关企业在开展数据信息安全防护工作时,还应该采用合适的技术手段,对其自身的信息储存容量予以扩充,使其储存虚拟空间变得更大,从而承载储存更多的数据信息,而储存空间本身就具备较高的安全防护能力,这就使得被储存在虚拟空间中的数据信息则会得到较大的安全保障。

3.2 加强对信息安全的监督管理

相关企业在经营运行过程中,若想保证自身以及用户个人的数据信息的安全性,严防其出现泄露问题,则需要对内部以及外部的数据信息加大安全监管力度,做好相应的防护工作,以防一些数据信息被泄露出去,影响到企业的运营或者个人的生产生活。与此同时,广大群众也应该参与到信息安全的监管工作中,对于一些不良商家以及企业予以积极举报,这样也有利于提高企业的责任意识及信息安全防护意识,进而形成良好的信息共享环境氛围,以此保障数据信息的安全性。对于大数据而言,其本身是一种新生的事物,因此,在法律规范方面缺乏完善性,网络上一些违法的数据信息行为,缺乏有利的约束以及规范,这就需要相应的法律制度对其进行严格规范以及硬性要求,通过这一方式实现对企业、个人信息的有效保护,使得相关数据信息的应用更加合理规范。大数据本身就来源于广大民众,所以,在维护信息安全的过程中,还应该注重提高广大民众自身的信息安全意识,这样也能够对一些数据信息安全风险进行防范,减少数据信息的安全隐患,从而在保护个人隐私、避免负面影响等方面产生重要作用。

在具体的信息安全防护工作中,相关企业可以对自主研发出来的、且具有较高安全系数的信息安全防护系统予以科学应用,借此提高自身或者是用户个人的信息安全防护水平,以免出

现内部信息泄露的现象。同时,相关企业也要加大内部监督力度,对于信息泄露这一问题予以严防严控,进一步保障内部信息的安全性。另外,针对外部信息的安全也要做好相应的防护工作。相关企业可以对APP予以自主研发,或者是针对原本的APP予以定期升级以及更新,对于自身APP的安全防护性能予以不断强化,以防APP受到黑客的攻击或者是网络病毒的入侵,保障数据信息不会被不法分子盗取,提高信息安全性,也能够促进企业的稳步发展^[5]。

3.3 加大对信息安全防护技术的研发力度

有关企业在对数据信息安全进行防护时,还应该对相关安全防护技术进行深入研究,以此提升数据信息的安全防护水平及能力。有关企业要认识到信息安全防护的重要性,对防护工作进行全面了解,在这一基础上,加大对数据信息的保护力度,对于非结构化的数据信息也要加以重视,并做好相应的安全防护力度,发挥出数据信息的重要作用,避免影响到企业的经营运行。信息安全防护技术的研发,需要充足的资金予以支持,因此,在开展技术研发工作时,相关企业应该加大资金投入。对于当下信息安全防护技术的研发现状及需求予以明确,结合实际情况,适时的投入一些资金,使其能够满足技术研发的实际需求,进一步推动技术研发进程。

另外,有关企业也要建立激励机制,针对在信息安全防护技术研发工作中,具有突出贡献的个人以及团体,给予一定的物质、精神奖励,比如,分发奖金、职位晋升、外出学习等等,借此激发相关科研人员的工作积极性,使其能够主动参与到技术研发工作之中,促使技术研发工作高效有序的开展。此外,相关企业在开展技术研发工作时,也可以与其他技术研发公司加强合作,要注重深化二者之间的合作深度,组织双方的技术人员开展研讨会,针对技术研发中的问题进行讨论交流,相互学习经验、解

决问题,降低技术研发难度,加快技术研发进度,提高安全防护技术水平。在具体的合作过程中,也要进行资源共享,比如,技术研发信息等,可以设置合适的实践活动,检验技术功能,由双方技术人员互相攻克信息防护系统,在这一过程中,寻找技术漏洞,针对具体漏洞进行技术优化,发挥技术作用。

4 总结

相关单位若想在大数据时代中,保持良好的发展状态,则需要将数据分析以及信息安全防护工作落实到位,减少信息安全风险,避免出现信息泄露问题,对企业单位的发展造成不良影响。相关企业单位也要提高对信息安全防护工作的重视度,并且要结合实际情况,采用合适的技术手段,对数据信息的安全性加以防护,以此降低企业经营风险的产生几率,促进企业的稳定发展。

[资助项目]

2022年度广东省科技创新战略专项资金(大学生科技创新培育)项目,大数据环境下的敏感数据脱敏技术研究,项目编号:pdjh2022b1090。

[参考文献]

- [1]张涛.大数据时代计算机网络信息安全及防护对策分析[J].世纪之星—交流版,2021,(14):2.
- [2]李福琳.大数据时代数据分析与信息安全防护[J].山东工业技术,2019,(6):1.
- [3]宋学莲.大数据时代计算机网络信息安全防护策略[J].计算机与网络,2021,47(14):49.
- [4]邱汤迪.大数据时代计算机网络信息安全现状及防护策略分析[J].科学与信息化,2020,(8):1.
- [5]侯凯莉,武心雨,陈莎莎.大数据时代计算机网络信息安全及防护策略研究[J].中国宽带,2021,(7):1.