基于大数据的信息安全框架策略分析

刘常

（武警兵团总队　新疆　乌鲁木齐　830000）

[摘　要]大数据已经逐渐渗透到社会生产生活的许多领域，成为新时期的生产力资源之一。相对于大数据技术的吃速发展和）、一泛应用，大数据安全技术并没有获得同步发展和长足突破，因此而带来的社会问题口益凸显。本文从大数据信息安全风险框架研究入手，分析大数据技术在应用过程中所面临的安全问题，从提升安全风险管理水平的角度，探索大数据信息安全风险的应对措施。

[关键词]大数据；信息安全框架；策略

【DOI】10.12252/j.issn.2096-6261.2021.05.464

1 大数据信息安全风险

大数据时代的信息安全所面临的挑战包括隐私信息的泄露，大量重要信息的大量储存同样也增加了信息泄露的风险指数。大数据包含的各种应用中支付宝、美团、滴滴出行以及携程旅行是人们在日常中经常使用的软件，这些应用的使用中会自动存储用户的各种重要的信息其中包括身份证信息、出行信息以及各种银行卡和账户余额信息，近几年用户个人信息被窃取的危险情况时有发生，所以大数据时代的今天关于信息安全的问题所面临的挑战并不简单。近几年黑客的出现严重破坏了网络信息平台的安全，现如今大数据的发展和探索也面临着被黑客攻击的严重危害。一些以贩卖个人信息来谋生的不法分子通过一些特殊的技术手段来潜入到各数据和信息平台的保密柜中进行网络信息窃取然后再以一定的价格进行倒卖，严重的时候可能窃取一个人的信息反复倒卖给很多人，这样就给被窃取信息的人的生活和生命产生极大危害。一些平台在关于信息技术的完善和创新中也存在很大的漏洞和危害，由于在一些技术中存在问题导致黑客通过木马程序种植很容易的盗取重要数据信息。大数据时代的信息安全所面临的挑战不只是技术手段同时还有系统方面的管理工作，一些平台或企业在关于大数据机构的管理人员的管理中也不系统，相关管理要求也并不完善，一些管理人员甚至还出现与社会上不法分子进行倒卖用户信息的违法行为。

2 大数据的信息安全框架策略分析

大数据正在逐步影响着国家治理、城市发展、企业生产、商业变革以及个人生活，但是大数据在给人们生产、生活带来便利的同时也带来了一些安全隐患。尤其是在互联网较为发达的今天，人们隐私信息的泄漏情况频发，例如人肉搜索、银行卡信息被盗等。所以，如何在大数据背景下提升信息安全就显得尤为重要。

2.1 数据存储技术

大数据的存储功能对信息软件要求较高，需要专业的人员进行定期的安全存储和维护，信息管理人员应注重利用云环境确保数据信息的安全。利用云环境对大数据进行存储，实现信息安全才是关键。例如可以采取对称与非对称加密计算方式，通过云环境实现海量数据的存储，很好地平衡大数据运算速度，才能真正解决安全存储问题。高效运用大数据统计作用，提升信息安全意识。例如可以建立安全管理制度、审计制度、应急响应机制，实现数据技术的全面应用和制度的落实才能确保信息的安全。例如在不明文件的弹窗下载中，用户应高度重视相关软件的下载，以防范黑客的不明攻击。用户应积极设置相关访问密码，并对相关具体案件进行学习，了解相关风险的危害性，才能真正的规避信息风险。工作人员应注重职业道德修养，积极在工作中坚持“保护用户信息安全”为原则，充分发挥数据信息技术的统计作用，将信息资源进行优势互补和全面整合，更好的提升安全防范意识，加强对相关网络信息案件的学习，才能真正通过大数据技术进行信息数据的高效利用。

2.2 数据分析技术

在大数据的视域下计算机的信息安全，在对数据进行处理的时候，所采用的一些数据分析技术，主要就是指在对数据进行实际处理的过程当中，使用计算机的人通过一些技术对数据进行分析工作，比如空间分析的技术、网络分析的技术、情感分析的技术、数据回归的分析技术等。在对一些案例进行大数据的分析的时候，其采取的主要技术就是数据分析的技术。在对一些数据进行实际分析的过程当中，空间分析的技术是把几种技术进行了相互结合，分别是地理数据的编码技术、几何技术、网络拓扑的技术，通过这种形式最终完成了对所有数据的综合分析。在使用网络分析的技术对数据进行实际分析的过程当中，一定要充分结合网络自身的优势，对数据进行处理分析。情感分析的技术就是指，把自然语言通过编码的形式呈现，进而去完成对数据的分析工作，可以有效防止在对数据进行分析的过程当中，出现一些安全事故比如数据信息的泄露。

2.3 数据加密技术

第一，匿名加密技术。匿名加密技术是当前密码技术中的研究重点，尤其是在大数据时代，大部分信息泄露的最重要原因是网络环境的相对开放性，所以，为了降低网络信息泄露，匿名加密技术的应用可以为用户营造一个相对更加隐秘和安全的环境，在保护用户隐私权益的同时，通过加密技术实现匿名，保护了用户在大数据网络环境下的信息安全。第二，同态加密技术。大数据包含的敏感信息量非常大，一旦出现信息泄露将带来严重的后果，即使脱敏之后信息，通过技术手段也能够被破译，因此对大数据加密是保护敏感信息的最有效手段。用户可以将需要处理的数据以密文的形式交给云端服务器，服务器可以直接对密文数据进行处理而不需要用户来解密数据，处理后服务器以密文的形式将处理结果返回给用户，用户收到处理结果后对其进行同态解街，得到已经处理好的明文数据，因此可利用同态加密技术对用户的隐私信息进行加密后存储在云端服务器上，其他用户只对有价值的信息进行处理，而不必知道用户的隐私信息。第三，可搜索加密技术。如何将加密文件存储到远程服务器同时又可以在保密的情况下实现数据检索和修改，就是可搜索加密的研究内容，也就是说可搜索加密是在加密的情况下实现数据检索功能。大数据一般都存储在远程服务器，但是远程服务器属于不可信赖的服务器，用户不想让服务器知道数据内容，此时需要采用可搜索加密技术对远程服务器上的数据进行加密处理，来增强数据的安全性。

3 结束语

大数据时代，数据信息安全风险备受关注，成为影响大数据不断扩大发展的重要阻碍因素。目前大数据信息风险比较多，对于用户的权益和安全影响较大，对此，需要尽快采取有效的措施来应对，注重用大数据的基础维护、技术措施、立法措施以及其他措施来提升安全风险处理效益。

参考文献

[1]周洪峰.大数据背景下信息通信数据加密技术分析[J].中国新通信，2020，22（03）：2-3.