大数据背景下信息通信网络安全管理管理策略研究

葛经纬
联通（浙江）产业互联网有限公司　浙江　杭州　310000

摘　要：在互联网以及计算机技术的支持下我国已经进入了大数据时代，各行各业在发展的进程之中更多的借助云计算技术慢慢完成了信息发展。在信息化发展的进程中，因为网络的开放性，促使信息通信网络安全工作面临一定危胁，安全隐患经常发生，并且还会对各行各业造成比较直接地不良影响。为了能能够确保信息通信网络的安全运营，为各行各业构建和谐生存与发展标准，本文对大数据环境下信息通信网络安全工作展开分析，希望可以为各行各业在发展中的信息安全性给予合理确保。

关键词：大数据背景；信息通信；网络安全；管理策略

引言

目前，我国经济发展快速发展的前提下，推动了我国信息通信网络的高速发展，使中国进入智能化互联网时代。在这样的环境下，对信息通信网络安全性有很高的规定。从现阶段生产建设情况看，为了能提高信息合理收集、实时监控系统及其精确传送的功效，各行各业基本上离不开通信技术，尤其是在日常日常生活，通信技术成为了大众的日常日常生活紧密联系的一种状态，不论是日常语音通话、和网络通讯互换作用的需要，或是日常基本生活保障的功效来看，通信技术已经肩负着信息交换、即时互通的桥梁纽带作用。由于对通信技术的需要，通信技术的科研投入也和日骤增，信息传输速度及其可靠性层面也逐渐有所提高。不难看出，为了能剖析在大数据环境下网络信息安全存在的问题，应建立相对应的思路，防止出现安全风险，合理推动大数据环境中的信息通信发展。

1 大数据分析技术和移动通信网络概述

1.1 大数据分析技术

信息化时代衍化了大数据分析技术性，提升了数据库的传送和融合速率，在这里数据信息爆发时期，大数据分析技术能从大量信息中挑选出有意义的信息，并详细分析应用到相符合情景。因为信息发生爆炸时代数据过多危害数据信息价值密度，想要在海量信息信息中获取到规格相符合变得十分艰难，因而，依靠大数据分析技术性，能通过关键字精确查找到目的数据信息，防止人为因素获取花费大量经济成本，提升数据的价值，为这一领域生产决策给出的数据适用。大数据分析技术性提升了数据处理方法高效率，还能够对获取过的有意义参考依据推行数据分析系统，提升数据信息信息的及时性与人化。

1.2 信息通信网络

信息通信网络包含移动互联网固定互联网，各个领域应用挪动通信网络比较广泛，原因是挪动通信网络能够不会受到时间和地点限定轻轻松松连网，提升客户上网体验感受。在我国现阶段挪动通信网络从原来4G升级成5G推广与应用，伴随着科技进步的高速发展，业内持续自主研发和产品升级，挪动通信网络服务水平将也不断顺从现阶段发展趋势，自主研发出更符合现阶段大家生产制造、生活所需的信息通信网络。伴随着人们对于通信网络市场需求的提升，信息通信网络还需要持续结合云计算技术，提升客户服务质量，保证信息通讯行业技术和国际性专业水准对接。

2 计算机数据通信网络安全维护要点

2.1 加密技术

在数据解决最为重要的是保障数据安全性和可靠性，所以在日常的电子计算机数据通信系统审核中，为了确保平安稳定性能，必须把加密技术置入到编号中，通过自己的密匙来确保数据安全性。传统加密技术一般由密钥和优化算法两方面构成，密匙主要是用于对数据开展加密和解密的独特计算方式，优化算法将收集的信息和密匙组成保密传递的数据。伴随着信息科技的迅猛发展加密技术也持续改善尤其是伴随着人们对于数据安全重视度不断提升加密技术早已广泛用于数据传送全过程。

2.2 防火墙技术

防火墙是安全设置的高效方法之一，具备十分强大的数据安全配置。在网络防火墙中，基本功能具有隔离的作用。是两个网络通讯时实施的访问权限方式之一。简单点来说，根据防护对数据的浏览被批准，没被批准浏览的数据的信息，释放出来得到浏览权的数据的信息的专业技术，能够最大程度地阻拦故意浏览。在数据环

境下，假如不设定防火墙技术，数据可以随意浏览，信息安全性无法得到合理确保，防火墙技术如同数据安全“防撬门”，务必为人民群众所高度重视

2.3 网络防病毒技术

互联网病毒安全防护技术性主要是针对各种各样病毒进行合理的安全防护，进而进一步提高互联网的可靠性和稳定性，保证数据的成功推广和接受。假如数据感染病毒，不但会危害数据自身安全性，还可能造成网络瘫痪。侵略计算机病毒主要分已经知道病毒和不明病毒。对已经知道病毒开展防止时，大家应依据病毒特性选择适合自己的防止方式。预防不明病毒时，大家理应采用动态性判断的方法，融合病毒的举动规律性对病毒进行分析和分析判断。一旦互联网感染病毒，在对待病毒时，一个是融合发生病毒的网站根目录，一个是马上防护感染病毒文件，降低其他资料感染病毒的几率，对病毒的感染范围进行有效控制[1]。

3 大数据背景下信息通信安全隐患问题分析

3.1 软硬件设施安全问题

在信息通信的过程中，软硬件建设是所有网络运作的一环。不论是在公司办公室或是在学习上，硬件条件都涉及到电子计算机、储存器、网络终端设备和通讯设备等多个方面。这种硬件配置存有安全隐患，比如受环境因素条件的限制，机器设备毁坏，运作时间太长造成机械故障等，在使用中会影响到信息通讯的总体品质。假如机器设备存有安全隐患，信息在传送过程中需要有泄漏、遗失的风险性，比较严重的时候会危害通讯网络的应用和业务的正常进行。手机软件在APP运用环节中通常遭受网络环境的作用，给全部信息通讯带来一定的安全风险。比如，病毒感染威协是最常见的软件平台难题之一，假如某一手机软件在安装及使用中置入病毒感染，可能会影响全部全面的正常运转，危害信息通讯网络的安全性。

3.2 缺乏完整的信息通信安全管理体系

近些年，因为信息通信安全难题高发，为积极应对信息通讯网络安全隐患，国家相关管理方法多部门联合本地机关事业单位设立了信息通信安全管理体系，增强了相关行业工作员对信息通信安全管理工作的安全防护观念搭建的信息通信安全系统软件遮盖不足，构建体系的相关介绍没法归纳各个行业，并没有我国法律约束，没法突发事件处理，一旦出现网络安全隐患，无法具有管理方法功效，给消费者和平台增添了不可挽回的财产损失我国现阶段的网络安全风险管理不够成熟，尚未产生全国各地统一标准，信息通讯网络安全生产工作欠缺高效的合作与协调，并没有健全系统软件专业的法律条文的管束相关部门在处理信息通讯网络安全性违法案件时，规范缺少所造成的处罚力度也受影响，对犯罪嫌疑人没法具有强有力的威慑和整治功效。

3.3 网络信息不安全

在互联网时代的大环境下，互联网技术掌握了各种各样信息，这种网络信息中不仅有安全信息，也是有不安全的信息。一些网民并没有辨别信息能力，不可以合理辨别信息真假，客户手机上网时，只有处于被动接受欠佳信息具体内容，明显减少了网民在网络条件下的体验感受，一些网络网络运营商除此之外，一些网站还存在着行骗、虚报信息，这种不安全的网络信息不但会给网民产生不必要财产损失，也让一些网民对大数据环境下信息安全性形成了怀疑。

3.4 信息通信防护方面不安全

在大数据环境下，网民总数逐步增加，越来越多网民遭受网络安全威协。在这么大量的信息数据信息环境下，要高效地确保每一个网络客户的网络信息安全并不是一件容易的事情。网络安全性数据调查报告，在信息通信安全评定中，安全风险评估升级速率迟缓，不能及时解决大数据增长，网络发生高危安全风险，造成网络客户信息泄漏。除此之外，信息通讯安全防护技术的应用相关人员的开发上要很长一段时间，短时间没法合理安全防护各网络客户的信息。

4 大数据背景下信息通信网络安全管理策略

4.1 管理制度方面

信息通信系统安全制度的建立就是为了能够确保业务流程系统优化且平稳地运作。尤其是在大数据时代背景下，因为数据的形成是大量的，因而仅有做好网络安全管理工作中才可以为信息通讯的安全性给予系统化的保证。有关主管部门理应强化和别的各个部门间的交流合作，融合不一样业务流程系统的特性、对信息通信安全的需求等多个方面来搭建更加全面的制度体系。此外，每个各个部门也要高度重视对安全工作技术以及规章制度等多个方面提升与更新，通过各种前沿的电子信息技术维护体系等营造良好的信息通讯自然环境[2]。

4.2 基于稀疏码多址接入的端信息扩展

针对通信系统基本建设而言，怎样全面提升信息传送安全性可靠性能，一直是研制的关键侧重点，近几年，以入侵防御技术性、入侵检测技术及其数据处理工艺为主的传动系统传统意义上的互联网防御力方式，可以在一定层面上为网络信息安全具有一些安全防护的功效，但考虑到它具有处于被动、静态数据等特性，无法

完全高效的解决即时变动的网络入侵，安全防范水平还亟待加强。

对于互联网通信中出现的一些安全风险，联系实际运用延伸出端信息振荡定义，便是采用任意、动态变化转变通讯过时了端口地址、传送时隙、IP地址、数据优化算法，用于侵略者，做到病毒防护效果。还有一种端信息拓展的形式，把数据信息开展计算，采用IP地址、连接端口号、通讯协议等信息编号组成产生数据信息的形式，各种各样端信息和传送数据不会有矛盾和关系，从而达到将传送信息开展隐藏功效。除此之外，也有端信息跳扩混和技术性，便是采用端信息拓展编码序列即时认证方法，做到高隐秘性前提条件基本中的快速振荡同步。

4.3 构建信息通信安全管理体系，做好信息加密工作

为了保证信息和通信安全管理方法的品质，就必须要有一套完整的管理方案，这样才可以遵循一切规矩的管理活动，而且有能力管理一切合乎制度和所规定的信息和通信。第一，做好终端设备数据加密工作中。因为一端与另一端的通讯，在接受前需先向信息开展数据加密解决，然后传输，才能保证数据传输给的准确性，并避免被捕获和控制。第二，连接点数据的数据加密。信息和通讯数据在传送环节中根据无线路由器、网络交换机和其它系统进行传送，所以需要在合同中提升认证数据长短、减少误码率、防止控制等控制方法。第三，要做好数据加密连接的工作中，特别是无线网络连接。在具体通信保障中，无线通讯以无线电波为主导，用途广泛，覆盖面积广[3]。

4.4 借鉴区块链技术经验维护通信安全

区块链技术在信息通信安全保护主观因素方面有突显功效，还可以在区块链技术影响下获得一定通信安全工作经验。比如，在短消息、微信等非及时性通信业务中，选用区块链技术能够对信息自动备份应做到数据加密解决，并且通过收义者密匙做校验后才能达到信息二次传送，这类信息传送方法和传统电子邮箱实际操作表层如出一辙，但区块链技术可以利用密匙身份认证提升了信息数据安全性，数据信息安全加密等级更高一些，合理确保信息通讯网络信息安全。区块链技术伴随着需求者的增加，作用逐步完善，现阶段区块链技术具有类似菜单栏目录技术性，完成频道栏目作用，能设固定不动代理商对各种实际操作完成密名实际操作，更为个性化。区块链技术通讯技术无需提供IP地址，能够适用线下通讯,而P2P通讯技术需通讯主体线上PK，而且需要通讯主体彼此与此同时把握IP地址前提下完成通讯作用。区块链技术中的密名实际操作相较于P2P通讯技术个人隐私安全确保更全面。

4.5 保证系统安全，完善防御功能

在确保系统优化运作层面，大部分公司及部分政府机构为了节约人力资源、方便管理，只是设定单一的公司计算机网络管理人员，未对管理员权限开展分类管理，从管理工作来说，一旦出现错误操作，非常容易对网络信息安全自我防御机制产生安全风险，加上外部故意侵略手机软件攻击，网络信息安全将面临危险。传统网络入侵通常是运用被进入应用系统本身存有安全防护缺点违法伪造网络连接设置，进入公司内部盗取互联网信息，乃至毁坏数据传输，散播电脑病毒，导致计算机网络偏瘫，直接和间接的引起各种各样互联网通信安全技术难点的产生。科学合理设置管理级别及其管理权限，在其中目地之一就是能够即时搜索、剖析网络漏洞及其互联网预防缺点，与此同时能防止黑客攻击、远程网络进入[4]。

结束语：总的来说，网络上的各种数据网络资源，包含大量商业秘密信息、公司信息及个人数据，一旦出现我国、单位和个人风险性，就必须要加强网络安全管理方法，促进产业成长，提升数据使用率。大数据、云技术涉及到数据发掘的处理方法和分析。伴随着数据量多、网络空间繁杂，最底层信息与通信网络安全隐患日益突显。在我国正处于快速发展的时期，解决与分析各种各样存放信息是数据科技的首要任务，大数据运用一定要和云计算技术紧密结合，合理溶解与处理各种各样数据新闻媒体。

参考文献

[1]李鹏举.简析大数据背景下信息通信网络安全管理策略[J].数字技术与应用,2021,39(05):184-186.

[2]阮旭东.大数据时代的信息通信数据加密技术[J].中阿科技论坛(中英文),2021(05):124-126.

[3]鲍俊如,熊亮.大数据下信息通信技术中的隐私保护分析[J].中国新通信,2021,23(08):15-16.

[4]何敏华.大数据背景下信息通信网络安全管理策略研究[J].中国管理信息化,2021,24(07):169-171.