分析数据加密技术在网络通信安全中的应用

邵立岩

中国人民大学 北京 100872

摘 要：在全民互联网的时代背景下，计算机网络中储存和传输的数据量随着时间的推移与网民用户的增加越来越大，这些数据中涉及普通信息、个人隐私、企业与单位的机密数据等等重要或不重要的信息资料。在未能采用数据加密技术或是没有增设其他安全防护的情况下显然很容易由于通信信息安全得不到保障，导致个人、单位或企业的数据泄露而引发社会事件。基于此，本文将着眼于数据加密技术与网络通信的含义概述来简要分析前者在后者中的应用价值、常用加密技术、应用方式等内容，期望能为数据加密技术与网络通信的持续发展提供一些浅知拙见。

关键词：数据加密技术；计算机网络；通信安全；应用

Analyze the application of data encryption technology in network communication security

Liyan Shao

Renmin University of China，Beijing 100872

Abstract: Under the background of the Internet for all, the amount of data stored and transmitted in the computer network is increasing with the passage of time and the increase of Internet users. These data involve important or unimportant information, such as general information, personal privacy, confidential data of enterprises and units, etc. Without the use of data encryption technology or the addition of other security protection, it is obviously easy to cause social events due to the lack of guarantee of communication information security, resulting in the data leakage of individuals, units or enterprises. Based on this, this paper will focus on the meaning overview of data encryption technology and network communication to briefly analyze the application value, common encryption technology, application mode and other contents of the former in the latter, hoping to provide some insights for the sustainable development of data encryption technology and network communication.

Keywords: Data encryption technology; Computer network; Communication security; Application

如果说人类的语言是文字，那么计算机的语言就是数字，也就是说数字就是人们在使用网络时计算机所接收到的信息。无论是线下的日常生活生产还是线上的互联网交互都会应用到数据信息，数据在如今信息化社会中已经逐渐成为核心内容。由此可见，对数据信息进行加密防护能通过大幅度提升网络信息的风险防控程度来保障人们的隐私安全，而如今在网络通信中最常用的一种安全防护手段就是能对传输数据进行加密的数据加密技术，可以有效防止信息泄露。

1. 计算机网络通信与数据加密技术概述

1.1 计算机网络通信概述

网络通信就是通过网络技术将独立的工作站或是主机连接起来进行数据信息的交互，通过一定的技术手段实现人与人、人与计算机、计算机与计算机之间的交流通信、资源共享等等。网络通信中最为重要的网络通信协议可以将之称为网络通用语言，主要凭借对信息传输代码、传输速度、传输步骤、出错控制等内容进行严谨规定来连接不同操作系统与不同硬件体系进行互联互通，进而搭建形成能连接整个社会的网络结构 [1]。

1.2 数据加密技术概述

数据加密技术就是通过一种技术手段将明文信息加密转化为无意义的密文后传输到信息的接收方，而接收方就会按照预先设定好的解密方式进行解密来获取特殊化处理前的信息，这一过程中出现的加密与解密方式可以称之为密钥。如今，有很多数据加密技术采用了能随时改变的动态密码来提高数据信息的安全防护质量，在增加破解者解密难度的同时为加密者增加了更多强化数据安全防护技术的时间。

1.3 应用价值分析

依托于互联网搭建形成的信息化社会带动各行各业转变原有的结构体系，实现了信息化管理、智能化改造、自动化加工等等，实际上这些转变过程就是将原有信息资料进行数据化的过程。因而加强数据安全防护能保护各行各业市场主体、单位与个人的信息安全，甚至很多国家机密数据信息如果缺失安全防护手段将会直接对国防安全、社会稳定性造成极大的威胁；而对于企业来讲，诸多商业信息如果在传输时被泄露的话就会直接影响企业的运行稳定性和经济效益。尤其是随着网络技术的进步，电子商务行业的诞生与发展促使很多企业纷纷开通了线上销售、签约、沟通渠道，而数据加密技术应用在电子商务行业等领域的网络通信安全防护中能够更好地满足其未来的发展需求，消费者与商家能够在足够安全的网络环境中足不出户地完成互动沟通和销售购买环节，且无需担心信息泄露风险 [2]。

2. 常用加密技术

2.1 链路加密

链路加密就是对网络通信链进行在线加密来保障信息传输安全的一种技术，数据信息会在传输之前被加密并在传输节点被解密成明文形式，然后这些明文数据信息又使用下一链路的密钥进行新的加密与节点解密环节，

在这一反复的加密和解密过程中会不断改变密钥以防有人劫取信息去破译解密。我国所公开的首例全链路安全加密技术是由阿里巴巴公司于 2018 年公之于众的，在其旗下的钉钉软件中发布了新版安全白皮书中将全链路安全加密技术进行公开以展现自身对用户数据信息的安全保护力度。在链路上以密文形式出现的所有数据信息能够掩盖信息的发出源点与终点，但也由于链路加密技术需要同步链路两端加密设备的这一特性使其面对一些信号不稳定的环境很容易出现数据丢失等问题，同时每个节点的安全维护也需要在人财物方面消耗大量的资源。链路加密技术中有一种身份密钥加密方式，如果在采用链路加密技术时仍然出现了数据信息被盗取的危急情况就会很容易破译信息，通常开发技术人员会在加密后端引进身份识别标志去防控这一环节所存在的风险问题，尽可能做到全方位保障。

2.2 节点加密

与链路加密操作方式相似但形式不同的一种技术就是节点加密技术，同样是将网络通信链路层当做载体的节点加密技术并不允许数据信息在节点中将其转化为明文形式，这项技术会在传输节点中的一个安全模块进行解密与加密环节来防控信息解密过程中的信息泄露风险。但是传输节点并非牢不可破的，如今 AI 智能时代的背景下大幅度降低了节点加密技术的安全防护效果，很多终端信息会受到 AI 自主识别机制的影响而被采集和破译数据隐私，针对这一情况就会采用动态加密与可验证技术等方式保障终端用户的信息主权。

2.3 端到端加密

这项直接连接两个终端的加密技术不会由于数据在传输时被解密而导致出现泄漏危机，并且还有着操作性简单、成本设计费用较低、实用性较强、节点损坏后不会丢失或失真数据信息等方面的优势，不过这很容易由于数据传输者的保密意识不强造成人为出现信息泄露的问题。端到端加密技术在数据信息的完整性、终端的同步性、传输过程的可靠性等方面都有着较高的安全保障，并且报文包也可以通过端对端加密技术进行独立传输以免链路或节点出现问题造成泄漏危机。

2.4 密钥加密

最为简单且便捷的数据加密方式就是密钥加密技术，直接采用专用密钥将加密密钥与文件绑定起来实现加密操作，接收者运用已知密钥进行解密。尽管泄露风险较高，但这项常用于实际文件传输过程中的数据加密技术无需使用者掌握较高的专业水平 [3]。

3. 数据加密技术在计算机网络通信安全中的应用

3.1 计算机软件

能驱动计算机发挥各种功能的计算机软件形式多样且难免出现漏洞问题，不法分子在攻击计算机获取信息时就会通过这些漏洞控制电脑进行犯罪活动，不法分子可以在获取个人或企业单位已储存重要信息的同时操控计算机登录各类软件来收集更多的信息资料。因此，在计算机软件中应用数据加密技术可以有效保障软件信息以免被窃取隐私信息或机密信息，通常普通用户对常用的计算机软件直接设置密码就可以完成基础加密操作，但如果是企业和单位想要进行更高强度的加密处理就需要使用计算机自带、专门下载或是聘请技术公司制作特殊的安全防护软件作为支持。不论是个人还是企业单位都需要定期对计算机软件实施病毒查杀去清理隐藏病毒以防泄露风险，通过此类形式能够有效保障计算机的运行安稳性以及个人隐私、企业单位机密数据信息的安全性。

另外，计算机下载安装软件时也会应用到相应的数据加密技术，例如说部分计算机自带的应用商店会要求输入相应的密钥才能完成软件下载操作；还有一些软件在下载时本身也需要下载密钥运行软件才能获取到安装解码密钥。软件作为人们操控计算机进行生活生产的必备用具受到不少不法分子的关注，一些软件下载平台就容易受病毒的攻击导致其中的软件在下载时会被同步植入垃圾软件或是木马病毒，直接影响计算机使用者的重要信息安全与计算机本身的运行稳定性。从用户的角度来讲，计算机软件作为一种娱乐消遣或是办公学习的必要工具具有极高的实用价值且储存了诸多隐私信息；而从软件开发商的角度来讲，计算机软件作为一种盈利工具能带来丰富的经济利润且其中信息关乎着自身的社会形象和地位。各类社交软件、网络游戏、线上购物平台等计算机软件如果使用人数多且热度极高就很容易吸引不法分子的攻击，利用数据加密技术可以保护用户的账户信息、个人隐私信息、支付密码等等数据资料以免损害消费者切身利益并维护软件开发商的综合效益。

3.2 数据库管理

储存了大量信息资料的数据库是计算机网络通信中容易遭受病毒攻击的主要系统之一，数据库管理系统已经逐渐成为各个政府单位与企业所引进应用的重要技术，结合大数据、云空间、云计算、人工智能等技术帮助企业单位更高质高效的管理愈发复杂多样的海量数据信息。数据库需要与互联网相连接才能实时收集企业单位所需的数据信息以及储存业务活动产生的大量数据信息，当数据库出现泄露风险时将会造成难以估量的经济损失并破坏企业单位的正常运行秩序。基于此，在数据库管理中应用数据加密技术可以实现分级平台化管理，能够针对不同程度的安全防护需求的数据资料运用不同等级的数据加密技术进行防护，对于更加机密的重要信息能够采用更高等级的防护来尽可能增加储存数据的安全性。互联网的共享特性促使以其为载体的数据库将要面临在公共空间加密储存的巨大风险，而通过验证密匙、用户访问权限等形式的数据加密技术能在一定程度上达到较为优质的数据信息泄露风险防控效果。

3.3 局域网

局域网作为一种封闭性强、安装便捷、节约成本、扩展方便且具备多种共享功能的、覆盖一定范围的网络种类能够有效保障企业单位的数据资料安全，国内拥有局域网的企业单位大部分都是国家相关单位、大型企业与基本搭建形成现代化管理结构的少部分中小型企业。在局域网范围内，企业和单位会应用到数据加密技术来保障内部通信需求与数据信息安全性，并且局域网的数据加密技术相较于覆盖面更广泛的大型互联网络而言安全防护效果更好。局域网的封闭性特征相当于为企业单

位内部传输的数据信息无形之中增加了一层安全防护手段，再应用数据加密技术能够对数据传输终端、链路、接收端进行加密以增强数据信息的安全性，同时也更好地限制了不法分子攻击企业单位数据库的恶劣行径。尤其是在当前市场经济快速发展和信息技术的高速进步的社会形势为中小企业带来了更大更多的发展机遇，而企业发展期间则会产生诸多有关员工、业务活动、战略规划等多个领域的数据信息，越来越多的企业开始搭建专用局域网络作为内部数据信息传输和运营管理的重要手段，一旦被病毒或是不法分子攻破将会由于大量数据信息丢失或泄露造成企业损失巨大且破坏其在客户心中的良好形象。因此，合理运用数据加密技术能够有效保护局域网内的海量数据资料的安全性，即使是局域网系统出现问题也能及时明确源头并做好防护处理来降低企业与客户损失 [4]。

3.4 电子商务

从电子商务行业来看，该行业的健康发展前景可以说是建立在足够安全可靠的网络环境之上的，而今在网络上频频爆出有软件或是商户贩卖消费者个人隐私信息导致出现了民众个人利益被侵害、财产受损等等恶劣影响，电子商务平台作为消费者与商家进行交易的线上空间必须保证基本的安全环境才能维护双方的利益，避免泄露商户的商业计划以及消费者的地址、电话、支付密码等信息造成利益和权益被侵害。在发展前景愈发宽广的电子商务行业中正经历着规模持续扩大的良好态势，从曾经的交易软件选购物品发展到如今直播平台式的线上推销购物的形式，在电子商务中应用诸如 SSL、SET 等安全电子交易协议以及数字证书、数字签名等形式的数据加密技术都可以有效保障消费者和商户的重要信息。另外，同样连接在电子商务平台中的还有各类工厂，工厂方面所产生的订单数据、订单总量等信息资料相较于消费者与商户企业之间更加庞大且复杂，因此，在线上支付方式应用愈发广泛的时代背景下将信息安全与财产安全之间划上了等号，一旦出现丢失、泄露等数据安全问题就很有可能造成大面积经济利益损失或是隐私权利被侵害。通常电子商务行业所采用的数据加密技术有身份认证、动态密码、生物识别、多模块加密技术等多种方式，直接提高了不法分子破解密码的难度和满足人们对数据加密的多样化需求。

4. 计算机网络通信安全的保障措施

4.1 建立健全网络安全管理机制

建立健全网络安全管理机制能够有效保障互联网行业的健康发展前景和制约企图借用互联网管理的漏洞进行违法犯罪的思想。在信息化社会背景下有必要结合实际发展情况与需求来加强网络通信安全的重视和管理力度，根据新时代的发展观思想与科技的研发方向去制定计算机网络通信安全管理制度并实时更新安全技术和管理观念，保障管理制度的前瞻性、完整性、严谨性与科学合理性。同时，在面对计算机网络通信产品时也要注意从内部结构和技术设计入手进行持续性更新优化以提升产品在数据安全防护方面的可靠性，特别是各行业企业在开发设计新产品的过程中必须要具备守法意识去遵守国家法律规定与行业规范，秉持着严谨的态度和责任意识来为用户提供更安全可靠的服务体验。

4.2 不断增强网民安全意识

不法分子的诈骗手段同样也在随着时代的发展和科技的进步而不断变化，就譬如说利用疫情防控、外卖快递、信用卡债券等等手段骗取网民信任来掌握其隐私信息或是支付密码。目前仍有很多网民缺少信息安全防护意识导致自身利益受损或是对网络通信安全技术知识掌握不充分、使用不正确，因此，有关部门应当着眼于宣传教育方面进行持续性网络通信安全防护知识的普法活动，利用各类互动交流平台与碎片化时间树立众多网民用户的安全防护意识来保障其生命与财产安全。当然，政府方面还需要从立法入手去强调在网络通信系统设计中增加用户账户保护程序的必要性，为网民提供更多保护 [5]。

结语

总之，我国信息技术持续发展的环境背景下逐渐开发出了更先进的数据加密技术，随着信息化社会和智慧城市建设进程的加快，覆盖范围更广、功能更强、数据资料更多的计算机网络通信领域需要安全防护性能更优异的数据加密技术才能维护数据隐私安全。在计算机网络通信安全防护中可以有选择性地采用链路加密、节点加密、端到端加密、密钥加密等方式保护数据安全，而数据加密技术可以应用在计算机软件、数据库管理、局域网、电子商务等各行业领域中保障多方利益，因此需要更完善的安全管理机制来提高网民安全意识才能更好地维护网络世界秩序。

参考文献

[1] 高杨 . 数据加密技术在计算机网络通信安全中的应用 [J]. 光源与照明 ,2021(06):43-44.

[2] 任钊 . 数据加密技术在计算机网络通信安全中的应用 [J]. 信息记录材料 ,2021,22(05):199-200.

[3] 吴文臣 , 郭伟伟 . 数据加密技术在计算机网络通信安全中的应用 [J]. 网络安全技术与应用 ,2021(04):22-24.

[4] 戴禄君 . 数据加密技术在计算机网络通信安全中的应用 [J]. 网络安全技术与应用 ,2021(04):24-25.

[5] 滕海军 . 计算机网络通信安全中数据加密技术的应用 [J]. 信息记录材料 ,2021,22(04):213-214.

作者简介：邵立岩（1990.01）男 满 辽宁丹东 本科 学生 研究方向：计算机应用技术