

论数据加密技术在计算机网络信息安全保障方面的应用

刘铭晓凡

青岛理工大学 山东青岛 266000

摘要: 随着信息化时代的到来, 计算机网络越来越发达, 计算机技术和网络技术也被广泛的用于各行各业, 计算机网络信息的安全如何保障也成为了当下社会人们热议的话题。密码泄露、账户安全、浏览信息隐私, 因为信息安全得不到保障在使用计算机时也给大家造成了很多困扰。为了保障计算机网络储存的信息安全, 越来越多的网络主体会在计算机网络中采用数据的加密技术来保障信息的安全性, 这是一种常见的信息技术, 主要是通过加密信息数据来增强计算机网络信息的安全等级。在本文我们会详细介绍数据加密技术在保障计算机网络安全信息上的具体应用如软件、商务、网络数据, 以及在应用过程中需要注意的问题, 并针对此进行分析和探究, 来提升数据加密技术在信息保障上的应用效果。

关键词: 数据加密技术; 计算机; 网络信息安全; 实践应用

引言:

近年来网络科技发展迅速, 村村通、5G网、4k高清的电影。我国的网络设施基础在不断的完善, 网络技术在不断的进步, 网络通信功能已经和人们息息相关, 计算机网络已经是社会的主要构成部分, 人们的吃穿住行都已经离不开它, 互联网更是成为大家生活中不可或缺的一部分。现在计算机网络被用于各行各业, 比如: 信息化的教育, 学校利用多媒体技术教学培养学生的主动学习能力; 看病不用去医院排队可以先在网上预约挂号, 你还可以打开浏览器输入你的症状支付1元钱就有名师帮你诊断, 药品还能直接送货上门; 还有现在的支付宝的线上支付乘地铁公交只需要手机的二维码扫一扫; 互联网和农业也是现在很新潮的应用, 代替原始的人力制造了电子设备, 可以节省更多的时间和人工, 计算机网络在已经成为人们在生活、学习、工作中最重要的使用工具。但在享受计算机给人们创造的高效便捷性的同时我们也发现了人们的安全信息保障还存在很多的威胁。比如电信网络诈骗、银行卡被盗刷、计算机病毒入侵、数据隐私被恢复、黑客非法入侵、计算机系统存在漏洞等一系列的问题, 这些问足以让我们在计算机引起足够的戒备心。为了保障用户的使用安全, 社会的持续和谐的发展, 我们必须通过数据的加密技术来增强计算机的信息安全保障能力, 抵御更多非法的人为操作引起的人们财产损失保障网络主体的信息安全。

一、数据加密技术

1. 什么是数据加密技术

(1) 数据技术加密原理

数据加密技术是一种保护网络数据的计算机技术, 主要是将在计算机网络中获取到的信息通过加密的手段如加密的钥匙或加密的函数将文字转换成没有任何意义的密文来进行传播, 当接收到信息的一方看到密文内容后再利用解密的形式把密文还原成原来的信息。开发数据加密技术就是为了保障网络在使用过程中信息传播的安全。

2. 数据加密技术的分类

(1) 节点加密

在数据传送方传输信息的过程中, 会利用一种特殊的加密场所, 在这个场所里进行数据传输, 传送接收信双方存在距离, 每段距离设计一个节点, 每段距离传输的信息量不同通常会在传输信息量最庞大的中间节点进行实时性加密。

(2) 链路加密

与刚才节点解密的原理相似, 就是加密两个相邻的节点, 因为传输的距离区段不同还有每次传输的场所不同加密得效果会有差异。这种加密形式在使用过程中能有效提升数据的安全性, 在数据传输时采用传送密文服务端明文的方法可以在始端末端隐藏, 因为一直处于加密的状态所以也能有效抵御病毒的攻击, 从而降低了计算机运行的危险指数。

(3) 双互加密

一般是传送方端口加密再运输到接收方端口解密, 双互加密就是端到端加密, 则是加密与解密在传送端口与接收端口的位置同时进行, 这样就能确保数据在传播过程中信息是全程加密的, 不仅操作方法简单而且信息

的安全程度更高。也是目前用的最多的加密方式之一。

3. 数据加密技术的特点

(1) 数据加工

这是最本质特征，对数据进行加工，把在计算机网络使用中接收到的所有人都能够辨别的数据信息通过特定的算法进行加工，再传播给只有少数人可以利用特定密匙解密辨别原文内容的数据信息。

(2) 算法复杂

转化的加密技术就是处理明文信息的一种过程，是需要精确地算法才能进行加密，不同的算法有不同的类别。算法类型不一样对应的计算方式也有所不同，产生的结果也截然不同。现在被人们常用的对计算机的加密计算方式有：置换表算法、循环位移、更换表算法、循环冗余校验算法等。计算方法相对复杂。

(3) 减少接触用户数量

数据机密技术是通过双发加密传输，数据传送方把数据信息通过特定的算法进行加密处理，再把密匙告诉数据接收方，数据接收方接收到密文后再通过得到的密匙破解从而可以获得密文信息。特定的密匙对应特定的密文，就像一把钥匙对应把锁一样。因为数据加密是双方通过特定的密匙双互传输可以大大减少在传输过程中的其他用户接触，信息安全保障大大提升。

二、计算机网络信息安全存在的问题

了解了数据加密技术操作原理和特点，我们再来看看计算机网络信息安全到底存在什么样的问题，才能在后期技术的运用上提升使用效果有更好的突破。

1. 系统有漏洞

计算机在使用过程中存在一定的漏洞，比如我们浏览一个网页就会有网页的历史记录或者浏览痕迹，网络黑客就可以通过你在计算机网络操作留下的上网痕迹入侵到计算的系统里面，找到系统的漏洞再趁机植入病毒，这样就可以控制住计算机的系统运作模式，盗取内部的储存信息占位己用，所以平时在使用互联网时要谨慎点击任何链接，不要轻易下载未知软件或者浏览未知的网站，同时还要安装好清理杀毒的软件及时更新防护。

2. 黑客入侵

在计算机安全使用过程中黑客也是极大的隐患，黑客在现在的社会中也成为了一种大家诟病的职业，他们通常是一些高级计算级技术人员，通过侵入电脑系统盗取用户资料来谋取自身的利益。前几天新闻就有报道，一男子由于航班延误引起不满，黑入航空公司的网络系统导致网络瘫痪几分钟损失极其惨重，这是一种违法犯

罪行为。所以职业黑客的存在对于人们的经济、安全、隐私都有极大的威胁。

3. 未知病毒

计算机在使用过程中也会常常遇到未知的病毒，就像人偶尔也有个头痛脑热感冒发烧的病症，这是无法完全避免的，一般常见的就是木马病毒和熊猫病毒，这些病毒一出现就会破坏计算机的运行系统，造成系统瘫痪导致很多加密文件被破坏或者数据信息被泄露。即使有计算机自带的防火墙或者是杀毒软件也没有办法阻止病毒的入侵。

4. 管理不规范

网络管理不规范也是现在计算机网络信息安全存在的一大问题。现在打开网页铺天盖地而来各种广告垃圾信息，一不小心点进去一就会中病毒，还有很多是赌博黄色的网站，严重的会导致很多用户上当受骗，财产身心受损，轻微的就是电脑黑屏系统崩盘数据丢失。这不仅威胁了用户的隐私安全还会占用大量的公共资源，所以计算机网络信息管理者还需要加大网络信息安全管理力度。

三、数据加密技术在保障网络信息安全方面的具体应用

目前数据加密技术在不同的应用方式和应用场景上对网络信息安全的保障呈现出多元化的状态。不是单一的而是变化多样的，我们可以针对不同的网络类型，不一样的应用环节采取不同的加密手段进行数据处理，来保障网络信息的安全性。那数据加密技术具体在计算机网络信息安全方面有哪些应用呢？

1. 软件加密

软件加密的主要应用就是我们常见的计算机杀毒软件，像360安全清理大师、鲁大师、电脑管家。这类软件不仅能对计算机网络中出现的病毒进行清除，还可以阻止未知程序的安装有效的防护电脑存储的文件信息。为了防止病毒入侵造成杀毒软件失效降低存储文件数据信息的安全性，一般我们会提前对杀毒软件的安全性和有效性进行检测，确定了保护信息的安全之后再对数据进行加密处理。

2. 系统加密

为了使用户在使用计算机时操作更简单，现在计算机一般都是使用WindowsNT系统或者是Unix系统，这类系统的安全性能较低一般是最低的C1和C2级别，因为系统自身的存储功能不强，所以容易造成用户在操作过程中用户的数据信息外泄或者存储的信息被篡改的破坏。

数据加密技术可以给操作系统设置权限，也就改变系统的操作指令，同时对存储信息的数据库进行技术性的加密，用户要进行访问操作时需要先获取对应的访问权限，这样不仅提高了整个操作系统的安全性，还能够减少系统被侵入的风险。

3. 网络加密

虚拟专用网络是一种可以通过服务器软件传输可靠消息连接大型企业或团体的通信方式，太过传统的单一的密钥很容易被破解造成数据文件的泄露，所以很多企业为了保证信息的安全性一般会构建局域网，通过设置网络防火墙，对局域网进行加密处理，通过节点端口加密上述我们讲的方法来保证数据传输过程中的安全保障能力。一般企业的路由器就有加密功能在对局域网进行数据加密技术，在对所有的文件、信息、数据进行实时加密，接收的路由器再解密转化成原来的文件，减少了接触人员数量同时还能规避文件泄露风险构建了更加安全的网络环境。同时通过局域网的数据加密技术可以实现局域网中不同区域的安全保障作用，能保证各项企业的业务能顺利实施。

4. 数据加密

数据加密技术在数据机密这块的主要应用是：网络数据库加密。计算机网络数据库是集中存储信息的地方，信息量过于庞大所以安全性能也必须是最高级，为了确保数据库里的各类信息数据安全除了对网络数据库进行加密处理外还需要对用户在使用计算机过程中的数据信息安全进行检验检测和防范。用户在进行计算机操作时会对用户的数据进行存储，加密的网络数据库就可以对这些数据进行分析检测，如果存在不安全的隐患，会自动转化到操作端显示给用户，用户接收到电脑的提醒再对此进行安全处理。

5. 身份认证

在过去的几十年里身份证是每个人身份识别的唯一标志，归属感极强，在当今的网络时代，为了确认用户的身份有很多认证方法，身份认证是目前运用最广泛的数据加密技术之一，在身份认证技术中主要有两种类别，一是身份认证二是网络身份认证，两者之间有区别也有一定得共同点。

6. 网络身份认证

用户在登录网络时需要提供自己的身份信息进行认证才能获得相应的访问权限。有三种模式分别是：动态密码、USBKey、OCL模式。

(1) 动态密码

动态密码安全性高，使用较多，主要是利用服务器和客户端时间差的特点来进行验证，这个在生活中也是随处可见，绑定银行卡、注册APP、设置密码等等。只动态验证码有语音动态码和数字动态码，只要客户端和服务器密码一致验证就可以完成验证登录成功。

(2) OCL模式

OCL是一种对象约束语言，施加在指定模型元素上的约束语言，是一种新型的身份认证技术方案，主要用于网上银行个人账户的安全系统操作认证，验证模式有很多种。比如利用动态口令和手动密码或者手机验证码和密码结合使用，最大限度保障了交易者的资金安全保障。

(3) USBKey

USBKey是一种有有存储空间内置智能芯片的USB接口的硬件设备。USBKey里内置的用户私钥经过数据机密技术上锁，加密锁主要用于软件破解和复制，防止软件被盗版，安全程度较高。

7. 身份认证

(1) 利用用户知道的信息

因为我们在进行计算机操作时会向系统提供自己的身份信息，所以在网络数据中有我们的身份信息。比如在登录qq、淘宝、微信时会让你选择，以下哪一个不是你的微信好友，或者设置密保问题，当你答对了问题才能完成验证。

(2) 利用用户拥有的东西

因为信息数据的存储，计算机网络已经掌握了我们的数据。比如在登录各种APP时都需要你动态的验证码，你能收到信息，同时还有让你拖动图标到指定位置进行验证，还有根据顺序依次选出屏幕上的物体等等。还要就是程序二维码也是用户拥有的独有的东西。

(3) 利用身份特征

这个就很好解释了，现在的手机都是使用面部识别或者指纹识别，数据机密技术还会用在人脸识别技术和指纹识别技术还有DNA检测技术，都是利用的用户独一无二的身份特征来进行检测。

四、数据加密技术在使用中需要注意的问题和解决措施

1. 用户安全意识度不够

高效发展的网络时代，很多人对于计算机的使用并没有掌握足够的知识，只了解一些最基础的操作，因为知识储备较少所以也很难发现计算机的信息安全存在的隐患，导致自己的数据信息受到安全威胁。所以我们应

该在学校进行网络知识安全的知识培训，同时在社区、企业多多开展电信网络诈骗的宣传、讲座，告诫大家不要轻易点击陌生链接谨防木马病毒，尽可能使用安全性能高的计算机网络，同时下载app时注意查看安全提醒，使用安全支付时一定要注意动态密码不要外泄，同时对于未知的软件网页需要申请用户权限时一定要仔细阅读。

2. 没有科学规范的使用

数据加密技术目前还有很多的发展空间，并不是万能的，不能解决所有威胁计算机网络信息安全的隐患，所以用户在选择数据加密技术时一定要找专业的人员通过正当的渠道购买并科学规范的使用。所以针对科学运用的问题，用户在使用计算机时需要选择安全可靠的杀毒软件，同时要定期给杀毒软件杀毒，保证计算机在使用时出现如病毒、漏洞、黑客入侵等安全隐患时能被杀毒软件快速识别。

五、结论

在本文中我们了解到数据加密技术在计算机网络信息安全中的具体应用，也发现了在使用中所存在的问题，

数据加密技术作为保障网络信息安全的重要手段，值得受到社会各界人士的关注。数据加密技术的使用不仅能净化网络信息完全的环境，还大大的提升了计算机的使用效率，让企业经济得到高效的发展，同时让人们的生活更加便利，实现全球通、村村通，拉近了人与人之间的距离。数据加密技术保障了科技的高速发展，现在的人脸识别、指纹识别，越来越多的高科技走进了人们的生活中，我们可以手机购物、手机支付、二维码乘车，刷身份证坐高铁，APP看病、5G通讯在线播放视频、汽车无人驾驶等等，网络让我们的生活变得更加丰富多彩。所以我们要科学的选择使用数据机密技术，确保自身的网络信息安全。

参考文献：

- [1]于家德.数据加密技术在计算机网络信息安全保障方面的应用研究[J].通信电源技术, 2021, 38(2): 3.
- [2]李效渊, 刘赛彬.数据加密技术在计算机网络通信安全中的应用[J].2021.
- [3]韩冬.数据加密技术在计算机网络安全中的应用[J].中国新通信, 2021, 23(19): 2.