计算机信息技术数据的安全漏洞与加密技术探究

陆周萍
绿城科技产业服务集团有限公司　浙江杭州　310000

摘　要：计算机信息技术数据的传输、使用、存储面临着各种安全漏洞，使数据面临窃取、破坏等风险。数据加密技术作为保护计算机信息技术数据的重要手段，能够最大限度提高安全漏洞防护效果。基于此，本文从实际情况出发，首先分析了计算机信息数据安全漏洞影响因素，进而阐述了计算机信息技术数据安全漏洞的主要形式，最后针对性提出了计算机信息技术中数据加密技术的应用，以供参考。

关键词：计算机信息技术数据；安全漏洞；加密技术

引言

信息技术的高速发展对社会各行各业的运行、生产模式产生了深刻影响，计算机信息技术已深入社会方方面面。人们在使用计算机信息技术数据的过程中面临着大量的数据安全风险，尤其是各类数据安全漏洞，使网络数据面临着非法访问、窃取、泄露的威胁，如果数据被窃取、遗失，则会对用户造成严重损失。对接计算机信息技术数据的安全漏洞类型，使用各类加密技术已成为加强数据安全效果的重要手段。通过加密技术的使用能够最大程度提高计算机信息技术数据的安全性，对打造安全的网络应用环境有着重要作用。

1 计算机信息数据安全漏洞影响因素

1.1 人为因素

信息技术的高速发展与应用普及，不断提升了计算机自动化水平，但在使用计算机设备的过程中仍需要人为地输入操作指令控制计算机设备。计算机设备在使用过程中，操作人员自身的应用能力和安全意识、数据使用的规范性都会直接影响计算机信息技术数据安全效果。目前常见的计算机攻击手段包括电脑病毒，计算机病毒的侵入一般是操作人员在执行计算机程序时没有注意异常数据，导致病毒代码混入正常数据中流入计算机系统，进而产生病毒破坏的情况。许多电脑病毒存在潜伏期，短时间内不会产生效果，而是在特定时间点迅速传播[1]。这些电脑病毒的植入会导致计算机收集数据信息的全面泄露和破坏，直接造成较为明显的安全漏洞。

1.2 其他因素

计算机信息技术数据安全漏洞的产生除了人为因素以外，也包括其他因素。比如，电脑安装程序本身存在安全漏洞，同样会导致病毒的侵入。相较与人为因素产生的漏洞，计算机操作系统本身具备的安全漏洞具有较高的隐蔽性，漏洞溯源难度大，漏洞产生的形式多样。如果不能及时修复，则会进一步加剧漏洞的扩散效果。非人为因素导致的数据安全漏洞，与计算机程序的研发、编程有着直接关系。参与研发的代码在运行、编程方面存在问题，产生安全漏洞，不利于信息的安全使用与存储。

2 计算机信息技术数据安全漏洞的主要形式

2.1 网页链接安全漏洞

信息技术的高速发展与普及，对社会各行各业的生产运行模式产生了深刻影响，信息时代下，信息数据已成为新的资产类型。尤其是计算机信息技术的不断下沉，人民群众对信息技术的使用依赖更高，使用范围更加广泛，也成为许多企业生产所必需的基本技术。在计算机信息技术的使用过程中，部分用户安全意识较为薄弱，缺乏对安全漏洞的正确认识，对数据泄露问题的认知程度不高，缺乏正确的防范方法，导致网页链接安全漏洞的产生。网页链接安全漏洞是一种伪装性的漏洞形式，将病毒隐藏在网页链接中，部分用户在使用计算机时对陌生链接缺乏防范，进入链接后导致病毒侵入，导致信息被盗、个人数据泄露。网页链接安全漏洞是一种较为常见的漏洞形式，用户需要警惕陌生链接，避免病毒侵入。此外，企业在使用计算机设备的过程中会储存大量生产数据、产品资料，这些信息数据是企业重要的资产，业务人员在使用设备的过程中如果点击了陌生链接，导致病毒侵入数据库找到企业的数据存放位置，则很有可能导致数据

丢失、破坏、篡改，使企业遭受巨大的经济损失。

2.2 黑客入侵安全漏洞

黑客入侵安全漏洞主要以黑客攻击的形式呈现，许多不法分子通过利用计算机设备的安全漏洞进行侵入，获取用户信息数据。高频次的黑客攻击甚至能够攻破防火墙，严重威胁计算机信息技术安全。可以说，黑客入侵安全漏洞是计算机信息技术存在的最为广泛、破坏力也相对最强的安全漏洞形式。黑客入侵的手段多样、破坏力强大，利用计算系统存在漏洞攻破系统，强制获取用户个人信息，甚至可以操控系统篡改信息。由于黑客入侵的方法较为多样，一般用户无法精准识别黑客攻击手段，在不易察觉的地方被盗取个人数据，对计算机信息技术数据使用产生了很大的安全威胁。

2.3 木马病毒安全漏洞

计算机设备在使用过程中需借助各类软件进行信息的存储、使用和检索。软件中的安全漏洞成为一大隐患。系统和软件的漏洞是木马病毒入侵的先决条件，而漏洞的不断蔓延极易引发数据泄露风险，计算机信息技术软件安全漏洞主要表现为病毒入侵和非法攻击两大方面。木马病毒不仅会衍生出了大量的网络病毒，且病毒的溯源难度也显著增加。木马病毒的传播速度极快，破坏能力强，对计算机网络安全系统的冲击力度也较为强大，受木马病毒侵袭所造成的不同程度损害，将直接导致用户个人数据面临泄露和破坏的风险[2]。高级木马病毒程序甚至会控制用户计算机，更改计算机软件程序指令，用户计算机中使用的所有数据信息都会被病毒收集。缺乏计算机安全意识和技术能力的用户，对木马病毒的识别、阻止能力较差。

2.4 防火墙安全漏洞

防火墙是计算机信息系统中重要的安全防护系统，具有阻挡病毒和黑客攻击的重要作用。但是从实际情况来看，防火墙安全等级和防护强度与技术水平具有直接关系。部分用户缺乏充分的安全意识，对防火墙使用的重视度不高。此外，一些防火墙本身的防护等级不高，防护能力较差，病毒很容易通过防火墙安全漏洞在用户没有察觉的情况下搜集数据信息。许多用户对防火墙的认识不深刻，使用低等级防火墙的同时过于依赖防火墙预警，难以掌握防火墙存在的安全漏洞，防火墙安全漏洞管理难度较高。

3 计算机信息技术中数据加密技术的应用

3.1 虚拟专用网络的应用

虚拟专用网络（VPN）是一种基于数据加密技术构建的虚拟专用网络，主要是通过远程接入、企业组网和匿名上网等方式应用于计算机信息技术数据安全防护。VPN 运行期间，会与开放的公共互联网搭建一条具有加密效果的数据传输通道，任何经过这条通道的数据信息都需要通过加密验证，未通过验证的数据则不能进入设备中。VPN 技术采用的加密算法是一种融合了非对称和对称加密的混合式算法，通过这种组合方式有效降低了开放互联网对数据的安全威胁，加密效果更强、数据传输效率更高。对称加密算法是通过公共密钥的方式，对 VPN 通道内数据信息提供加密支持，对称式加密具有加密效率高、加密速度快的特点，能够满足大规模数据传输的性能要求。但是由于密钥的一对一共享模式，密钥的管理、分发难度较大，任何使用数据的用户都需要获取密钥。因此，在对称加密技术中结合使用非对称加密算法，能够在实现大规模加密数据传输的基础上，通过 VPN 加密通道安全地交换密钥。

企事业单位是 VPN 技术使用的主要场景，尤其是涉及跨区域业务的企业事业单位，可以利用 VPN 点对点的加密方式实现不同地区分支机构的加密互联，构建出满足企业业务高质量开展的企业专网。这种加密网络的全面构建能够实现总部与分支、分支与分支之间的安全互通。总部员工、分部员工只需要接入 VPN 加密通道就能相对高效、安全地连接企业内网，并实现数据的高效交互与应用[3]。普通用户日常使用计算机设备时也可以通过搭建 VPN 的方式来加强防护安全效果，尤其是在陌生网络上传输数据时，可以通过 VPN 隐藏 IP 避免受到网络追踪，为用户信息数据安全传递、高效传递奠定基础。

3.2 超文本传输安全协议的应用

超文本传输安全协议（HTTPS）是一种应用范围最广、安全防护作用范围最大的一种加密技术，是 Web 应用中使用相对广泛的一种安全通信协议。HTTPS 主要是在计算机网络应用层 HTTP 协议和传输层 TCP 协议中间的传输部分加入安全套接字层，应用层到传输层所流通的所有数据都需要验证信息完整性并做好身份认证。HTTPS 采用的混合加密机制较为灵活，能够在保障信息数据传输效率的基础上保障数据的安全性。HTTPS 建立连接后，将触发 SSL/TLS 握

手过程，这一过程是传输端与接收端的交互过程。在握手过程中，后续通信使用对称加密算法进行密钥交互，有效解决了非对称算法密钥共享较难的问题。非对称加密计算量大，数据信息传递速度较慢，但是具有更高的安全性，一般在机密文件、重要文件传输应用中应用较为广泛。非对称算法的加密针对客户端使用公共密钥，而私人服务器在使用数据时需要使用私钥才能解密，即便数据信息被不法分子截取，没有私钥也无法破密信息。密钥交换完成后，HTTPS 的信息数据传输通过结合对称加密和私钥技术进行数据加密，能够实现大规模数据的加密处理。

与此同时，HTTPS 同样引入了数字证书技术，为数据使用传输双方的身份认证奠定了基础。目前来看，数字证书的 PKI 体系较为灵活，包括证书认证的跟进范围、证书颁布的数字签名、服务器域名、私人服务器私钥等各类信息。数字证书技术使用期间，需要对数据流经的服务器域名、服务器加密公钥进行判定，避免 DNS 劫持、病毒侵入等攻击 [4]。HTTPS 在运算性能上具有显著优势，但同时也会增加计算机用户在通信时延、加密计算上的成本开销，尤其是 SSL/TLS 握手过程需要使用非对称算法和对称加密算法，加密、解密、证书验证耗费的时间成本、计算成本更高。在计算机硬件设备不同阶段升级的过程中，SSL/TLS 握手过程所需时间持续缩短，同时得益于 HTTPS 的性能优化，在证书验证、加密数据传输等过程中的性能损耗也进一步降低，整体发展的安全性、成熟性大大提升。目前来看，HTTPS已成为企事业单位Web应用所使用的标准加密技术，如网上银行、企业邮箱、社交媒体等软件都开始大规模使用 HTTPS 进行加密，对于保护隐私数据和机密数据的安全传输、遏制网络威胁均有着重要的积极影响。目前来看，下一代HTTPS/3标准已成为Web网络安全加密的重要发展方向，未来 HTTPS 也有望突破 Web 网络限制，为工业互联网、物联网等更多网络应用场景提供加密支持，为实现“万物互联”目标奠定基础。

3.3 区块链技术的应用

区块链最开始作为比特币挖掘的底层算法，并没有直接用于网络安全加密方向。随着信息技术的不断发展以及网络的不断普及，区块链所具备的块链式存储、不可篡改、安全可信的去中心化分布式等诸多功能优势使其迅速成为一项全球性技术，并广泛运用于计算机信息技术数据加密工作中。区块链技术通过密码学原理构建出一套维护数据可信的技术方案，区块链之所以能保证严格意义上的数据不可篡改的原因在于其采用了一系列密码学技术，包括哈希算法、非对称加密、共识算法和椭圆曲线数字签名算法。与其他加密技术相比，区块链技术融合的算法逻辑和技术手段更多，巧妙地融合了密码学、共识机制、分布存储等技术手段，使区块链从根本上保障了数据信息的不可篡改性 [5]。目前区块链技术正处于快速发展阶段，在大范围加密普及及隐私保护、技术监管方面仍面临诸多挑战，实现大规模商用也需克服一系列技术难题。但从现有情况来看，区块链作为一种全新的密码学应用实践，已成为计算机信息技术数据加密发展的重点方向，为互联网信息基础设施建设提供了全面的数据支持，也为计算机信息技术数据的高机密传输和不可篡改的信任构建提供了宝贵的创新探索。

4 结束语

综上所述，信息技术的飞速发展与快速普及对社会各行各业都产生了深刻影响。目前来看，计算机信息技术数据的使用、存储等方面存在一系列安全漏洞，对数据安全产生了严重威胁。使用一系列数据加密技术是保障计算机信息技术数据安全的重要方法和技术支撑，只有合理应用、高效使用各类数据加密技术，才能构筑出完善、坚实的网络安全防线。对接新时代发展特点，紧随网络安全形式变化，合理应用各类加密技术，打造出更高效、和谐的网络应用环境。

参考文献：

[1] 卜骁男 . 基于电子信息区块链技术的计算机数据安全保护策略探究 [J]. 中国安防 ,2025(05):87-90.

[2] 孔慧媛 , 郭文婷 , 李云 , 等 . 计算机科学技术在网络信息传输与数据存储中的应用 [J]. 软件 ,2025,46(02):86-88.

[3] 王莉 , 姜磊 . 大数据和智能控制技术在计算机网络信息安全系统中的应用 [J]. 网络安全和信息化 ,2025(02):134-136.

[4] 董洪蒙 . 计算机网络信息安全中的数据加密技术应用及防护策略 [J]. 造纸装备及材料 ,2024,53(10):130-132.

[5] 靳恒清 . 混合数据加密技术在计算机网络信息安全中的应用研究 [J]. 网络安全和信息化 ,2024(09):121-123.