网络通信中的数据信息安全保障技术研究

马德旺
中国联合网络通信集团有限公司北京市分公司　北京　100038

摘　要：信息系统的安全性是保证所有网络通信安全的关键因素。为促进我国网络信息安全，有必要对实时信息管理系统进行监控，并进行定期制度。扫描并修复网络通信中的安全问题。在信息管理系统中，不仅需要提供可用性，还需要增加安全性。所以，相关管理人员应合理配合，实现信息系统管理与网络通信安全的平衡，防止因我国网络信息系统带来的损失。

关键词：网络通信；数据信息；安全保障；技术应用

引言

网络的开放性使得用户在网络通信过程中容易受到病毒或黑客的攻击，从而导致个人信息的泄露和不必要的损失。所以，加强网络通信中的信息安全势在必行。针对当前网络通信中信息安全面临的风险，网络从业人员、相关管理部门、用户等各方应高度重视，提高网络信息安全技术水平，完善相关管理，增强安全意识，增强安全创造和谐与和谐网络通讯稳定的网络运行环境。

1 网络通信中信息安全保障的重要性

在通过网络传输信息的过程中，保证信息传输过程的安全性和完整性是非常重要的。现阶段网络信息技术发展速度非常快，应用领域不断扩大，渗透不断加深。尤其是在移动金融和移动支付方面，给人们的生活带来了极大的便利。但是，事实是双向的，在实现实时准确信息传输的过程中，网络通信也存在信息泄露的高风险。营利性犯罪分子利用从网络通信中窃取或泄露的个人信息实施网络诈骗，窃取网络用户财产，给个人的财产安全造成了严重的威胁。另外，一些恶意软件厂商或网络恶意泄露网络用户的个人信息，给用户造成严重损失。在这样的网络通信环境下，加强信息安全迫在眉睫。通过提供网络通信信息安全，最大限度保障网络用户的信息安全，营造和谐健康的网络环境，有效规避网络安全风险，减少因网络信息泄露造成的用户损失，推动现代网络技术的可持续发展。

2 网络通信中的数据信息安全保障技术

2.1 信息安全技术CP-ABE-CKM

现阶段，密钥加密是网络通信中信息保护最有效的一种技术方法，其安全性非常高。但是这种方式在具体的使用过程中，偶尔也会发生私钥泄露、属性僵化的问题，从而影响了通信安全。

在这个过程当中，一些研究人员提出了一种私钥隔离技术来改进私钥管理，但由于该技术的权限结构过于复杂，该技术的可行性较低。所以，人们又提出了CP-ABE-CKM技术，这是一种共享密钥管理协议技术，简化了技术架构，降低了解密开销，增加了技术的可行性。总体而言，该技术运营模式的支撑架构包括数据拥有者、产权、数据使用者、云存储中心、解密服务器等部分。该架构实施时，数据所有者将用户需要传输的信息转换为密文，就地传输并存储在对方的云存储中[1]。之后，属性管理器检查数据用户的属性集，确认该属性集满足密文访问策略，然后解密服务器用私钥对密文进行解密，以便用户访问密文，进而实现密钥管理的隐私性。

2.2 防火墙技术

防火墙技术现已被普遍运用互联网通信当中。防火墙技术能够通过控制远程信息来阻止对远程信息的访问，还能够有效地从外部网络中识别内部网络信息。提供针对未经授权和受感染的病毒以及当前 Internet 的安全性，这种方法效果较为显著。所以，有必要加强对防火墙技术的研发与创新，不断提升病毒防护与防火墙阻断功能。还应当及时更新的防病毒程序。为确保网络连接的安全性能，利用防火墙技术能够有效阻止恶意入侵，或者使用防火墙来限制端口。监控协议在保护信息以供用户在网络通信中更好地使用方面也发挥着重要作用。您可以找到用于记录和监视计算机的协议，从而保护网络通信并阻止没有通过授权的访问和病毒的风险。

2.3 信息安全技术 ARP-CP-ABE

网络通信管理中，属性加密技术主要是利用属性确定用户的身份信息。当用户需要访问信息是数据时，系统能够把属性的内容和访问方式进行比较分析，如果信息匹配成功，则授予访问权限。由于该方法不使用用户

的身份信息，所以，在身份验证过程中不会泄露用户信息，提高了网络通信的安全性。然而，在网络环境中，用户的身份并不能在短时间内保持不变，因为用户的角色和号码是实时变化的。因此，在实现属性加密时，可以使用 ARP-CP-ABE 技术随时撤销某个属性集的内容，以处理用户属性的变化，从而拒绝访问所需的用户。该技术的架构可以分为四个角色部分：数据所有者、云存储中心、所有权和数据用户[2]。其中，数据所有者是一种用户：最初拥有数据的用户，数据用户是有权访问数据的用户，所有权是分发密钥和管理所有属性的实体。 .系统中，云存储中心是密码机构的存储和分发中心。

2.4 CCP-ABE-BA信息安全技术

CCP-ABE-BA数据信息安全技术的价值在于形成了网络通信保护体系的主观能动性。在解决网络通信中的私钥泄露问题时，不仅要遏制该问题的影响，还要对恶意用户进行跟踪，以有效抵御恶意入侵和攻击，提高信息保护效率。该技术最大的特点是可以在保护用户身份安全的同时，追踪攻击者的身份。总的来说，该技术的支持模型的架构组件与CP-ABE-CKM技术的组件相同，都是包含解密服务器和属性权限的五个对象。该技术在进行恶意用户跟踪时，系统会根据上述通用架构建立一两个安全模型。即CCP-AEB-BA选择文明攻击模型，CP-ABE选择文明攻击模型。利用攻击模型及其使用，将恶意用户抽象为敌人，同时抽象出挑战者，实现游戏模式下恶意用户信息的可追溯性。

3 网络通信中的数据信息安全保障措施

3.1 开展网络信息安全培训，提高用户安全意识

加强网络通信中信息安全保护是非常重要的一项内容，一是提高网络用户的安全意识，在使用此类网络技术工具时，要注意自己的隐私，严格规避风险。信息泄露。因此，有关部门应重视推动网络用户网络信息安全培训的实际实施，通过各种媒体渠道加强网络信息安全宣传宣传，增强了网络用户的安全理念[4]。与此同时，通过有效开展信息安全教育，使我们充分认识非法浏览网页造成的严重危害，自觉抵制非法浏览网页。另外，通过认识到各种防火墙和杀毒软件的重要性，不关闭防火墙，增加了网络病毒对个别系统攻击的可能性，有效地培养了用户正确使用电子设备的习惯，保持良好的使用状态。

3.2 增强通信协议 TCP/IP的保护的安全性

在从网络环境中窃取用户网络信息的过程中，犯罪分子通常会获取用户的IP地址，然后对用户的网络发起恶意攻击以窃取用户的信息。所以，有必要加强TCP/IP通信协议的安全性。在TCP/IP协议的结构中，二层交换机主要是实现高效的信息传递，因此需要加强对交换机的保护和控制，加强对用户IP地址的保护。另外，通过对路由器的隔离和监控，可以对IP地址的访问进行监控，在对异常IP地址的访问后，可以及时进行拦截，有效防止不法分子通过攻击用户的方式窃取信息。

3.3 注意定期保养

在我们拥有大量数据并且可以执行高效操作之前，我们需要注意维护我们的计算机系统，以便尽快检测到硬件故障的迹象。以路由器、交换机、集线器等设备为代表的网络互联系统，可以高效地进行网络传输和连接。如果设备出现故障，相应的指示灯会改变颜色以提醒用户。

所以，在平工作与学习中应当加强注意设备指示灯的状态[5]。如果灯框颜色发生变化，必须立即通知相应的技术服务部门，并及时确定错误原因并进行维修。另外，要特别注意信息的保存，对于重要信息要进行妥善保管，做好备份，以备不时之需，尽量避免不必要的损失。

3.4 优化病毒检测与预防

计算机病毒很可能对网络通信系统造带来一定的破坏。计算机网络安全的主要目标是能够很好地检测和对抗病毒。防火墙技术能够有效保护计算机免受传统特洛伊木马病毒侵害，确保了网络的安全性。这不仅增强了游戏的安全性[6]，还能够有效保护应用程序免受网络威胁，保护网络通信免受黑客和木马以及所有监视攻击。病毒扫描软件还可以更准确地识别特定的木马病毒，让用户立即清除病毒，有效减少与网络通信相关的威胁。在使用病毒检测软件时，通常会使用特殊的方法来确定计算机病毒造成的损害类型。例如，是否自动重启电脑。这将显示所有计算机上的病毒。用户应使用此表格进行病毒检测和清除，以提高网络通信的过程中安全性能。

4 结束语

综上所述，在信息技术发展的背景下，企业和个人都应增强网络信息安全意识，特别是专业的网络技术人员，在对计算机网络系统的主动监督管理中，应做好本职工作，加强监管， 要识别硬件系统设施信息管理系统的隐患，完善工作职责，并且确保各部分始终保持相互协调配合，除此之外，还需要建立健全完善的监管网络，确保我国网络系统的运行安全，推动网络系统平台

的稳定运行。

参考文献

[1]官月月,郭建勤,张胜平.网络通信中的数据信息安全保障技术研究[J].无线互联科技,2021,18(16):3-4.

[2]屈强.新时期网络通信安全分析及安全防护策略[J].科学与信息化,2021(23):97-99.

[3]查志勇,余明阳,詹伟,等.网络通信中的数据信息安全保障技术分析[J].电子世界,2020(24):55-56.

[4]王岩松,袁永涛,周磊.网络通信中的数据信息安全保障技术分析[J].科技创新导报,2020,17(03):130+132.

[5]曹怡.通信安全与信息系统管理安全探讨[J].行政事业资产与财务,2021(20):103-104.

[6]燕雯霞,刘会芳,张瑾.网络通信中信息安全的保障措施研究[J].数字通信世界,2021(03):152-153.