基于区块链的计算机通信网络安全评价研究

顾海康

兰州博文科技学院，甘肃 兰州 730100

摘　　要： 在网络社会中，人们的生活、学习、工作和娱乐都离不开网络的参与。然而，在人们享受计算机带来便利服务的同时，计算机通信网络安全问题也变得越来越突出。一旦通信网络遭到病毒入侵、不法分子的破坏，用户的生命财产安全就会受到不同程度的损失，严重影响了社会的和谐、友善发展。本文分析了计算机通信网络安全评价内涵，发现影响通信网络安全的主要因素集中在三个方面：病毒、人为因素、资源共享。为此，本文从四个方面对计算机通信网络安全防护策略进行了初步探究。

关 键 词： 区块链；计算机通信；网络安全评价

Research on Security Evaluation of Computer Communication Network Based on Blockchain

Gu Haikang

Lanzhou Bowen College of Science and Technology, Lanzhou,Gansu 730100

Abstract: In the online society, people's lives, studies, work, and entertainment cannot be separated from the participation of the internet. However, while people enjoy the convenience services brought by computers, the security issues of computer communication networks have become increasingly prominent. Once the communication network is invaded by viruses and damaged by criminals, the safety of users' lives and property will be affected to varying degrees, seriously affecting the harmonious and friendly development of society. This article analyzes the connotation of computer communication network security evaluation and finds that the main factors affecting communication network security are concentrated in three aspects: viruses, human factors, and resource sharing. Therefore, this article conducts a preliminary exploration of computer communication network security protection strategies from four aspects.

Keywords: blockchain; computer communications; network security evaluation

在信息化潮流时代，互联网、物联网得到了快速的发展。不过，随之而来的网络通信安全问题，严重影响了个体、企业使用网络安全性。为此，越来越多的用户在使用计算机网络通信时，都开始注重网络问题的安全性，普通用户会定期对防火墙、杀毒软件进行升级和病毒查杀，从而提高网络通信使用的安全性。

一、区块链背景下计算机通信网络安全评价内涵分析

（一）区块链背景下的通信网络安全评价模型

计算机通信网络一旦受到外来攻击，其内部信息必然会出现丢失、损坏等问题。[1]因此，需要高级网络技术人员对网络安全开展定量分析，构建完善的区块链计算机通信网络安全评价模型。模型架构包括信息管理（网络信息收集、网络信息中心、网络信息提供）、安全识别（创建网络安全、项目账本、汇总网络安全信息）、安全评价（主成分分析、创建安全分析账本、安全评价指标体系）以及安全报告（安全态势、智能合约、安全关联树）等四个部分。

（二）设计网络安全评价标准

在对计算机通信网络安全进行评价之前，需要高级网络技术人员建立完善的计算机通信网络安全评价标准体系。在设计评价标准体系时，应当立足网络安全识别结果、常规通信网络安全标准，结合安全评价目的和需求，建立递进式安全评价体系。[2]例如，将安全评价体系分成三个层级：目标层、准则层和指标层，每个层级再设计九个具体的指标，如目标层下面可以设置信息丢失、信息篡改、信息损坏、服务中断、硬件缺陷、软件缺陷、通信协议缺陷、信息泄露、防火墙受损等。通过这些具体指标，可以大大降低影响通信安全的不确定性和模糊性，提高安全防护效果。

二、区块链背景下影响计算机通信网络安全的主要因素

（一）计算机病毒

计算机病毒是最为常见的计算机通信网络安全影响因素。计算机病毒的入侵，会直接导致用户系统和软件失控、数据信息丢失等情况的发生。同时，在网络中隐藏的计算机病毒多种多样，而且防不胜防。[3]这些计算机病毒一旦完成网络入侵，一部分会去破坏计算机的原生系统，另外一部分则会对合法用户的文件数据信息进行破坏。例如，寄生型计算机病毒，这类病毒会寄存在电脑系统当中，非法占用大量的文件或是系统存储空间，导致用户无法正常存储信息。并且这些寄生型计算机病毒，还会不断在磁盘中传染病毒，占据越来越多的空间。计算机病毒的入侵过程十分隐蔽，大部分计算机用户很难察觉到计算机病毒入侵行为，当他们发现时，计算机病毒已经获取到非法用户所需的数据信息文件。为此，用户在使用计算机时，必须定期进行病毒查杀，才能够保证自身通信网络的安全性和私密性。[4]

（二）人为因素

虽然用户安全意识和网络通信安全之间的联系十分紧密，但是，在区块链背景下，仍旧有部分用户在对计算机网络通信进行使用时，安全方案意识缺乏十分薄弱，很难分清哪些网站是携带病毒的，哪些网站的绿色健康的，随意浏览病毒网站的行为，大大提高了网络系统安全问题的隐患，最终导致个人、企业数据信息的泄露和丢失。另外，随着信息技术快速发展，病毒消杀、防护的难度系数也越来越高。[5]而且不少非法用户为了得到更多的非法收入，他们会不断制造各种各样的计算机病毒，进而借助这些大量的新型网络病毒，攻击目标用户，将窃取到的信息进行兜售，从而达到非法盈利的目的。严重情况下，一些黑客会让用户的计算机网络陷入瘫痪当中。所谓黑客，是指一批具备超高计算机水平的网络罪犯，他们对计算机的使用手段、方法远远高于普通计算机用户，因此，他们设计和传播的病毒，往往不容易被 用户发现，严重影响了公众网络信息数据的隐私性和安全性。[6]

（三）资源共享

资源共享是区块链技术中的重点组成之一，通过资源共享可以实现不同用户对内部信息的使用和查询。同时，计算机软硬件中可以储存大量的丰富的数据信息，进而提高了资源共享质量和效率。[7]但是，资源共享技术的存在，在增加了通信网络开放性的同时，也增加了数据信息传输时的安全隐患，导致系统防火墙无法有效对网络各个节点进行鉴别和管理。一旦某个节点出现网络安全问题，不仅会导致系统网络无法正常运行，还会导致整个数据库出现信息丢失、信息错误现象的发生，严重损害了个人、企业财产安全。即便内部网络系统具有较强的安全防护措施，但是大量的开放节点，也会阻碍安全防护措施发现安全问题的时间和效率，使得安全问题持续扩大，不断增加个人、企业财产的损失程度。所以，高级网络技术人员必须要认识到资源共享的特点和重要性，创新技术管理手段和方案，加强各个共享节点的安全防护措施，保证数据资源的有效共享的同时，更要保证数据的安全性。[8]

三、基于区块链的计算机通信网络安全防护策略

（一）升级网络安全技术，强化防火墙作用

密码技术主要由对称和不对称两种加密技术构成。密码技术的本质就是一种信息的信息的伪装。密码类型共计有三种类型，依次是乘积密码、代替密码和移位密码。[9]其中，乘积密码从密码编码的角度来看，它比其它两种组成密码方式更为强大。乘积密码的原理是按特殊的规则将明文分成若干小段，并分别给每一小段乘以一个密钥，最后将乘积结果相加即可得到密文。众所周知，防火墙的作用是防止网络病毒入侵，也是保证网络安全的常规手段之一。防火墙技术，一般包括代理技术、应用网关和数据包过滤技术。它在计算机中的主要作用是控制某个网络的入、出权限，并强制对所有操作、连接进行检查，从而杜绝病毒入侵。因此，防火墙技术具有鉴别和限制外来数据流的功能，从而保证内网通信的安全。[10]当中的鉴别技术，可以对外来数据流的复制数据、篡改数据以及非法传送行为进行示警，并做出相应的安全保护措施，有效保证了各类网络信息在交换过程的真实性、合法性和有效性。常见的鉴别技术包括身份鉴别、数字签名以及报文鉴别。在信息技术发达的今天，用户在使用网络过程中，必须定期对网络安全技术或是软件进行升级，才能够更好地保护个人隐私信息。[11]

（二）利用实时网络，搭建安全策略

在保护网络安全过程中，不少用户都会设置用户访问权限，如身份鉴别、口令和密码等，以此来确定使用网络系统用户的真实性。在互联网日益发达的今天，用户也可以利用网络的实时特性进行网络授权，通过网络管理的方式核实终端访问用户的权限或是真实性，如有效口令、发放访问许可证书等，有效杜绝非授权用户使用内部网络或是盗用网络资源。[12]在利用网络进行实时安全管理时，仍旧需要注重加密机制的作用，它的存在可以让未授权用户无法看到真实的网络信息，切实保证了用户内部数据的安全性和保密性，有效杜绝了非法窃取行为的出现。同时，用户加强自身网络安全的过程中，还可以构建完善的数据鉴别机制，防止授权用户对内部资料进行修改、插入和删除，进而做好内外部的网络安全工作。[13]

（三）提高系统性能，及时进行应对

在设计计算机通信网络时，除了考虑安全防护措施外，还应该将各种安全因素纳入到考虑范畴中。例如，在初步设计网络系统时，就需要考虑到数据保密难度、通信软件系统和通信协议等环节的网络安全性能。同时，用户在使用网络通信时，应当逐步考虑和制定必要的防护措施和安全鉴别等级，从而减少系统漏洞、软件漏洞出现的几率，减低网络攻击者借助漏洞入侵网络系统的频率。[14]

（四）加强内部网络安全教育和管理

想要保证计算机网络的安全性，不能一味地依赖计算机通信安全技术，还需要认识到“人”在网络安全中的重要作用。计算机通信网络安全可以有效减少来自网络非法用户的攻击，但是，无法杜绝内部人员的网络入侵。因此，为了更好地提高通信网络

的安全性，不仅要对技术层次进行加强，还要对高级网络技术人员进行网络安全教育和管理，切实加强各部门之间协作，强化高级网络技术人员敬业精神，构建线上线下一体式网络安全“防火墙”。[15]

四、结语

总而言之，不可否认通信网络的发展，切实改变了人们的生活和工作方式。但是，在外部环境越来越复杂的今天，内部通信网络的安全也变得“岌岌可危”了。因此，为了降低病毒入侵网络风险、节点传输风险，高级网络技术人员必须升级安全防护技术和加密技术、强化自身职业精神，不断净化网络环境，才能够保证计算机通信网络的安全性、真实性和稳定性。

参考文献：

[1] 李薇. 基于区块链的计算机通信网络安全风险评估［J］. 信息技术，2024(002)：048.

[2] 吴小迪. 基于区块链的计算机通信网络安全加密控制系统设计［J］. 信息记录材料，2022，23(11)：163-165.

[3] 佚名. 区块链隐蔽通信方法，系统和计算机设备：CN202311829368.4［P］. 2024-01-30.

[4] 许浩敏. 基于区块链的计算机通信网络安全加密控制研究［J］. 长江信息通信，2023，36(5)：162-164.

[5] 邹佛新. 基于区块链的计算机通信网络安全加密控制系统设计与实现［J］. 电脑编程技巧与维护，2023(7)：167-169.

[6] 徐正平. 区块链的网络通信方法，通信装置及计算机存储介质：CN202110881078.9［P］. CN202110881078.9 2022-03-29.

[7] 张静，苏蓓蓓，黄星杰，等. 基于区块链技术的计算机网络安全优化方法［J］. 企业科技与发展：上半月，2022(000-003).

[8] 柴梦竹. 基于区块链技术的计算机网络安全优化分析［J］. 商情，2023(51)：0137-0140.

[9] 王近涛，黎楚. 基于主客观协同的区块链安全感知研究［J］. 计算机与数字工程，2023，51(6)：1348-1351.

[10] 邹福泰，谭越，梁晓实，等. 一种基于区块链的多域身份认证管理系统及方法：CN201910512296.8［P］. 2019-09-27.

[11] 邹福泰，徐源，王帅，等. 一种基于区块链的可信身份管理系统和方法. CN201811258603.6［P］. 2019-02-22.

[12] 荆博. 基于区块链的数据存储及通信方法，装置，设备和介质：CN202310222462.7［P］. 2023-04-11.

[13] 刘云. 基于 DNA 特征和区块链的数据网络传输安全保护方法及计算机可读存储介质. CN201811644826.6［P］. 2019-05-14.

[14] 唐菀，张艳，杨喜敏，等. 引入区块链的 SDN-IoT 网络安全：架构，方案与挑战［J］. 小型微型计算机系统，2022(010)：043.

[15] 徐军，姜奎，张宗宇，等. 大数据背景下基于区块链技术的高校网络信息安全模式研究［J］. 湖北第二师范学院学报，2023，40(2)：5-10.