基于区块链的网络安全体系结构与关键技术探究

王亚楠
（武汉商贸职业学院，湖北 武汉 430205）

摘要：随着互联网技术的发展，网络安全也引发了人们的关注。文章简述了网络安全体系结构的设计原则，分析了区块链的网络安全体系结构与关键技术。区块链技术的发展为网络安全体系结构提供了新的解决思路，有望成为促进网络安全体系革新的全新手段。

关键词：区块链；网络安全体系结构；关键技术
doi：10.3969/J.ISSN.1672-7274.2023.02.009
中图分类号：TP 393.08　　**文献标示码：**A　　**文章编码：**1672-7274（2023）02-0024-03

Research on Network Security Architecture and Key Technologies Based on Blockchain

WANG Ya'nan
(Wuhan Vocational College of Commerce and Trade, Wuhan 430205, China)

Abstract: With the development of Internet technology, network security has also attracted people's attention. This paper briefly describes the design principles of network security architecture, analyzes the network security architecture and key technologies of blockchain, and the development of blockchain technology provides a new solution for network security architecture, which is expected to become a new method to promote the innovation of network security architecture.

Key words: blockchain; network security architecture; key technology

1 网络安全体系结构的设计原则

1.1 保密性

网络系统中通常会存储很多信息资源，信息资源按照其类型进行划分，不同类型的信息保密要求也有所不同。设计人员在设计过程中需要考虑到不同级别的信息保护方案，避免信息非法泄露等问题出现。

1.2 完整性

在设计数据库时，通常需要加入身份识别、使用权限控制的安全控制手段，针对数据库使用者的身份和权限进行辨识。同时还需要保证每一份数据信息都支持备份和恢复，一些重要信息更是需要进行容错保护处理，最大限度地保证数据信息安全。安全性防护需要贯穿信息使用的全部周期，而且网络安全体系结构本身也需要具备一定的敏感性，保障信息的安全性与完整性。

1.3 可控性

对于网络安全体系结构来说，应当保证用户在实现信息索求、获取信息存储服务的同时保证网络信息的安全性与可控性，让用户可以结合自己的意愿对信息进行编辑和传递等。同时网络安全体系结构也要在用户索求信息过程中得到目标信息，提升信息的可用性。

1.4 安全性

需进一步提升网络安全体系结构的访问控制力度，针对内部用户的权限进行界定，对不同权限的用户的操作进行监控。同时针对不同的资源进行访问操作限制，全程进行审计和记录。根据网络安全体系结构的使用要求来设计对应的访问审计制度和控制制度。

1.5 时效性

网络监控系统是网络安全体系结构中的重点，当内部出现信息泄露问题时，需要及时发警报并进行处理。同时利用权限设计方法切断内部网络和外部系统的互联。针对业务上的外联线路，可以设计对应的管理体系，达到报警与制止的目的[1]。

基金项目：武汉商贸职业学院2021年度校级教科研项目立项课题“基于产教融合的计算机网络技术（网络安全方向）的人才培养改革研究”。
作者简介：王亚楠（1986-），女，汉族，河南南阳人，研究生，研究方向为计算机网络。

2 基于区块链的网络安全体系结构与关键技术

2.1 区块链在网络层安全中的应用

对于TCP/IP来说，网络层是实现数据安全传输的关键，利用控制平面及数据平面来指导流量转发，所以网络层安全需要重点考虑控制平面与数据平面的安全设计。目前区块链在网络层数据安全方面，一般利用协同式网络入侵检测系统，也就是CNNIDS，利用其控制网络流量，在发现流量异常时可以第一时间警报，保证网络数据安全。CNNIDS一般设计在多个区域，通过协调运作的方式来检测复杂的数据安全风险，而且反应十分灵活且迅速，能够对攻击流量进行过滤。基于环境信息同步的CNNIDS可以在系统间共享本地检测出的环境信息，每一个独立的入侵检测系统都能掌握环境信息，从而实现同步性的网络流量检测，其思路如图1所示。有关学者曾设计了一个基于区块链的协同式网络入侵检测系统框架，利用报警信息交换层和共识层来支持系统运作，前者主要负责报警信息的传输，后者则是确认报警信息是否一致。后续在该系统框架之上还加入了激励机制、新人管理机制等，建立了一个相对完善的报警信息平台，平台上的单位可以结合信用评分来订阅报警信息，激励参与者共享报警信息，并实现内部节点的安全管理。在这一平台中，参与方可以利用智能合约的方式来共享报警信息，也可以通过与信息发布者建立联系来接收报警信息[2]。

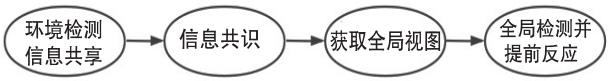

图1 基于环境信息同步的CNIDS思路图

基于模型信息同步的CNIDS系统如图2所示，这种系统能够在检测系统之间共享本地检测模型，在模型数据上实现共识。系统能够从区块链中筛选模型并获取一个具有检测功能的模型。

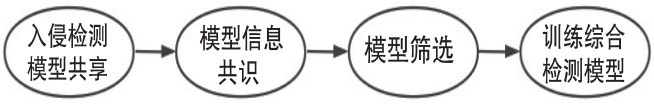

图2 基于模型信息同步的CNIDS思路图

从当前的情况来看，基于区块链的CNIDS系统一般将区块链视作一个分布式的存储平台，从而达到信息共享的目的。但和其他区块链应用中交易存在判别标准不一致的情况。而SeeCL平台的做法能够很好地解决这类问题，综合用户的评价进行模型筛选，但这种方法在每次采纳数据之前都要等待评价投票，所以时效性可能不尽如人意。此外还有一种解决方案，就是在真实存储的条件下加入真实激励，通过激励机制和应用层结合，按照参与者的行为记录评价其信用，根据信用评分来设计采纳策略，用户可以随时选择想要的数据，无须在其他用户评价之后选择。

2.2 区块链在应用层安全设计中的应用

2.2.1 漏洞检测众包

漏洞检测任务众包一般是软件供应商提供资金，由黑客进行检测并上报漏洞，最后根据上报的漏洞信息来修补漏洞，提高软件的安全性。软件供应商首先会发布一个漏洞赏金计划，其内容主要包括适用软件范围和赏金范围等，而黑客可以利用特殊平台来找到并接取赏金计划，按照赏金计划的要求进行软件测试，在发现漏洞后上报，最后软件供应商对漏洞报告进行审核，审核通过后为黑客提供赏金。漏洞检测众包能否顺利运作取决于软件供应商的诚信度，但从实践的角度来看，个别供应商却在修复漏洞后拒绝提供赏金，这可能造成信誉问题。同时漏洞赏金的设计本身并没有严格的标准，如果赏金额度较大，可能会提高预算支出；如果赏金额度较小，则难以顺利众包漏洞检测工作，甚至导致漏洞被扩散利用。在执行期间，单点信任问题并不少见，当多个黑客提交了重复的漏洞报告时，软件供应商可能难以处理，这也可能滋生出一些投机取巧的现象，例如，恶意参与者可能利用抄袭伪造的方式从中牟利[3]。

区块链的应用可以为漏洞检测众包提供一个真实的激励平台，实现激励机制和智能合约层的有效融合，将漏洞赏金作为激励手段，而且提高赏金发放的透明度，避免传统计划实施期间可能出现的单点信任问题。软件供应商可以通过智能合约的方法发布赏金计划，黑客也可以通过智能合约来提交漏洞检测报告，智能合约可以自动鉴别报告的真实性，而且自动从供应商的账户中扣款，让执行过程更加智能化、透明化。

2.2.2 访问控制机制

在大数据时代下，边缘计算和物联网的融合使得智慧城市得以实现，也衍生出了越来越多的应用服务，这些服务在为人们提供便利的同时也给访问控制带来了巨大的压力。新型服务相较于传统的网络服务来说，更加适合人们的日常生活，但其中的安全隐患同样不容小觑，甚至会给用户带来更加严重的经济损失。所以设计一套更加安全、更加可靠，能够保障用户隐私安全的访问控制机制就成为现实需求。

访问控制模型一般根据身份、角色、属性、能力等

进行访问控制，这种模型的应用已经越来越普遍，但这一模型在运行期间通常为中心化架构，部分应用在获得权限、访问用户信息时其实并不透明，这也是困扰很多软件用户的共性问题，用户并不知道自己的哪些数据被收集，也不知道何时被收集，更不知道信息用被在了何处。同时在云存储数据共享下，用户的信息存储和访问控制全权为云端负责，这可能会出现单点信任问题，在大数据背景下人们愈发关注自己的隐私信息，所以传统的访问控制机制存在的问题也显露无遗[4]。

若按照访问控制保护的主体差异，基于区块链的访问控制机制可以简单区分为三种：第一种为针对共享数据的访问控制；第二种是针对物联网设备的访问控制；第三种则是针对公共服务的访问控制。重点便是第三种，目前关于区块链的研究大多为基于区块链真实计算的特性，建立一个访问控制平台，数据提供者通过交易的方式将自己的信息共享，同时附加权限。数据消费者在请求访问时，智能合约可以实现权限的辨识，之后反馈回对应的数据信息，数据消费者每一次访问都会在区块链中留下记录。数据提供者所共享的信息被密钥加密处理，所以这种方式能够保障用户的信息安全。

利用区块链的功能性来建立访问控制平台，能够让访问控制变得更加精准且透明化，访问控制的结果也更加可靠。对于边缘计算服务器等公共资源来说，利用真实激励的策略可以规避恶意行为对资源无限访问的情况。虽然区块链在访问控制中的应用可能会造成一些成本问题，但可以将访问控制流程进行拆解处理，将区块链作为真实存储平台，主要进行全新信息的存储与更新、编辑等，权限验证则交由区块链的下游用户自行进行。但这种方式也有一些弊端，例如用户可能不具备执行访问控制流程的设备，所以需要根据不同的场景和需求来设计访问控制思路，平衡安全性与成本效益[5]。

2.3 区块链在PKI安全中的应用

PKI指的是公钥基础设施，主要负责公钥的创建与管理等工作，并且针对公钥持有者进行身份背书，实现用户之间身份的认证。PKI是网络安全基础设施中的重要构成，是网络安全体系结构运行的根基之一，在区块链的基础上可以实现算法的第三方查验证。此外，在证书颁发机构CA的监督与激励上，若只建立一个监督平台，那么警醒和惩处力度难免有些不足，所以需要利用PKI平台为CA提供更多奖励，从而鼓励更多参与者加入到CA操作监督的行列。这种方案效果尚佳，但在认证方面应当具备合法自愿，审计平台证书链通常仅保护证书状态信息的最新版本，同时为参与者提供证书查询等服务，这种方法能够避免证书透明机制CT以及证书撤销清单CRL等机制可能造成的单点信任问题。但这种操作其实并没有将区块链的真实算法特性发挥出来，证书的认证依然经过客户端来实现，证书账本Certledger则运用区块链的真实计算特性实现了预先计算，让原本的证书检验卸载到区块链，通过比特币简易支付的方法提供了客户端证书验证快速通道，但因为证书账本Certledger需要保存全部的凭证操作信息以及凭证状态信息等，所以内存消耗过大也是一个需要考虑的问题。PKI一般建立在信任网络上，利用使用者之间签署的协议来支持自身的运作，并且规避对CA的高度依赖，可以为普通用户提供交互式服务。但去中心化的PKI可能会面临一些安全问题，例如，证书状态与信任签名的传输可能会存在安全性或效率性问题。在去中心化PKI系统中，用户存储少数信任CA的证书，从CA维护站点中获取证书撤销信息，就能够验证证书的可靠性，但去中心化的PKI系统中的凭证分发机制以及撤销机制都为用户自主提供，若不加入中心节点则无法保证全部的证书状态信息都能安全稳定地传输出去。通过区块链技术构建分散式PKI，能够鼓励更多新用户加入，这有助于问题的解决[6]。

3 结束语

随着物联网、互联网、5G技术不断发展，信息共享也在潜移默化中影响着人们的生产生活。但网络安全威胁却不容小觑，寻常的杀毒软件以及防火墙技术并不能应对越来越严峻的网络安全形势。区块链技术的应用就很好地解决了这些问题，借助不对称密码技术来达到更好的安全防御效果，在实现数据与信息共享的同时，加强网络安全的自动化管理、自动化修护等功能。■

参考文献

[1] 陈科羽，石安安．基于区块链的网络安全体系结构与关键技术研究进展[J]．信息与电脑（理论版），2022,34(10):218-220.
[2] 徐恪，凌思通，李琦，等．基于区块链的网络安全体系结构与关键技术研究进展[J]．计算机学报，2021,44(1):55-83.
[3] 王群，李馥娟，周倩．网络空间安全体系结构及其关键技术研究[J]．南京理工大学学报，2019,43(4):495-504.
[4] 吕旻．网络安全体系结构的设计原则与实现方案研究[J]．自动化技术与应用，2017,36(6):82-84.
[5] 王洪亮．基于计算机的网络安全体系结构及技术的研究[J]．中小企业管理与科技（下旬刊），2015(9):257.
[6] 雷宇．IP网络内容安全分析系统体系结构及关键技术研究[D]．北京：北京邮电大学，2009.