

基于区块链技术的网络信息安全访问控制方法

张 锐¹ 黄 晋¹ 汪 希¹

ZHANG Kai HUANG Jin WANG Xi

摘 要

网络信息种类繁多、信息量庞大,传统访问控制方法仅关注单一系统或平台内的信息安全,忽视跨链信息访问控制。这导致攻击者可能利用跨链漏洞进行非法访问和数据窃取,严重威胁信息安全。为此,提出一种基于区块链技术的网络信息安全访问控制方法。通过区块链平台收集公共和私人事件参数、随机参数以及属性集,为访问控制提供数据基础。根据用户身份编号在属性中心验证身份,并将私有密钥转换为公有密钥,确保只有授权用户可访问特定信息。信息拥有者可设定访问策略,加密解密存储地址。采用特定的访问地址控制方法确保访问的安全性。对于多区块链信息间的访问,通过提取和验证多区块链间的共识点身份信息,确保访问请求的有效性和安全性。实验结果表明,所提方法的访问控制精准度高、空间消耗低,具有较高的实用价值。

关键词

区块链技术;网络信息;安全访问控制;密钥准备;授权中心

doi: 10.3969/j.issn.1672-9528.2024.09.045

0 引言

随着计算机网络技术的广泛普及和应用,信息系统成为支撑社会运转的重要基础设施,但同时也面临着来自黑客、病毒、木马等网络攻击者的严重威胁。这些攻击可能导致信息泄露、系统崩溃等严重后果,对个人、企业乃至国家安全构成极大威胁。因此,研究网络信息安全访问控制方法,旨在通过明确和限制用户对系统资源的访问操作,有效保护信息资源的机密性和完整性,成为当前网络安全领域的重要课题。

现阶段,研究人员不断探索新的访问控制技术和策略,以应对各种潜在的网络安全风险。文献[1]计算用户的访问频率,提取最高频率访问信息的特征值,通过双向映射使得用户减少对访问服务商的信任依赖,重新计算不同信息的储存开销并对泄露风险最大点进行加密,实现访问控制。这种控制方法虽然在一定程度上提高了信息安全性,但由于缺乏对跨链信息访问控制的有效机制,泄露风险最大点的加密可能不足以应对来自多个区块链的潜在威胁。攻击者可能通过多个途径尝试突破这些加密点,进而窃取敏感数据。文献[2]提出了一种以ABAC模型为基础的访问控制方法,对区块链进行形式化定义,划分场景并给出标签含义,建立访问规则库针对每一个访问用户在规则库中进行查找,完成域与域之间的访问控制。在该方法中,传统的ABAC模型主要关注单一

系统或平台内的属性匹配和访问决策,对于跨链信息的访问控制可能不够精确。文献[3]提出了一种增强NEDAC-MACS安全性方案,用于抵抗攻击,通过形式密码分析和性能分析表明,该方法能够保证前向安全性和后向安全性,与云存储环境相比,跨链信息访问控制需要更复杂的策略和机制来确保数据的安全性和隐私性。

由于缺乏对跨链信息访问控制的有效机制,跨链传输的信息可能面临更高的泄露风险。攻击者可能利用跨链信息交互的漏洞,窃取或篡改跨链数据。文献[4]引入密钥生成中心概念,提出信息访问控制协议,该协议具有可操作性,但是同样存在访问控制误差较大的问题。

针对上述方法存在的弊端,本文提出了一种基于区块链技术的网络信息安全访问控制方法,该方法专注于跨链环境下的信息安全性。该方法首先基于用户在不同区块链下的行为特征,对区块链平台参数、信息拥有者以及信息访问者进行细致的访问参数准备。在此基础上,通过创新性地提取和验证多区块链间的共识点身份信息,不仅显著提升了访问控制的精准度,还极大地增强了系统的安全性和可靠性。

这种跨链访问控制的方法不仅克服了传统访问控制策略在跨链环境中的局限性,而且为未来的网络信息安全领域提供了新的思路和解决方案。

1 网络信息安全访问准备

在访问控制前,对网络信息的安全访问进行参数准备。

1. 成都工贸职业技术学院 四川成都 611730

区块链技术的去中心化特性避免了单点故障和数据篡改的风险,提高了系统的稳定性和安全性。针对区块链中不同区域信息的特性,通过密钥管理和访问控制策略,可以实现对网络信息的精准控制,防止未经授权的访问和数据泄露。

(1) 区块链平台的参数准备

采用区块链平台搭载的生成机制获取 (G, G_T, g, e) 。其中, G, G_T 表示公共事件、私人事件^[5]存储参数; g 表示调用参数; e 表示随机参数。同时, 获取属性集 $\{A, \bar{A}, t\}$ 。其中, $A, \bar{A}$ 表示属性分量; t 表示时间。 $\{G, G_T, g, e\}$ 在区块链中以公共事件进行存储; $\{A, \bar{A}, t\}$ 在区块链中以隐私属性事件进行存储。

对区块链中所有属性信息进行初始计算, 采用循环群^[6-7]计算公钥参数。计算 $A, \bar{A}$ 的值可为访问者提供信息属性相关密钥, 并构造相关用户参数, 为访问控制判决做准备。

(2) 信息拥有者访问的参数准备

用公式 (1) 表示区块链中发布者参数:

$$P = \{X, \bar{X}, Y, \bar{Y}, Z_1, \bar{Z}_1, Z_2, \bar{Z}_2\} \quad (1)$$

式中: $\{X, \bar{X}, Y, \bar{Y}, Z_1, \bar{Z}_1, Z_2, \bar{Z}_2\}$ 表示区块链中信息拥有者参数, 可帮助建立访问者密钥, 实现精准访问控制判决。其中, $X, \bar{X}, Y, \bar{Y}, Z_1, \bar{Z}_1, Z_2, \bar{Z}_2$ 可通过上述过程求得的区块链公共参数以及循环群求解得到。 $X, \bar{X}, Y, \bar{Y}$ 可描述信息拥有者在区块链中的密文参数; $Z_1, \bar{Z}_1, Z_2, \bar{Z}_2$ 可描述信息访问者在区块链中的密文参数。信息拥有者参数准备可避免在安全访问加密过程中信息对权威中心^[8-10]的过度依赖, 保证每一次访问密钥都安全可用, 实现信息隐藏策略下的安全访问控制判定。

考虑到网络信息的种类较多、基数较大, 可能存在信息离散问题^[11], 需要信息拥有者在进行加密后再传输, 并在信息对应的区块链中标记该信息的加密信息, 保证安全访问控制的完整性, 加密信息构成的表达式为:

$$D_u = \{A_d, H_v, T_u, C, P\} \quad (2)$$

式中: A_d 表示信息加密地址^[12]; H_v 表示加密尺度; C 表示泄露风险; T_u 表示信息拥有者的访问属性集合, 其中包含多种信息属性, 如无关属性、隐私属性^[13-14]、公开属性以及真实属性等。

(3) 信息访问者的参数准备

$$R_k = \{D_0, \bar{D}_0, D_u, \{D_i\}_{1 \leq i \leq k}\} \quad (3)$$

式中: D_0 表示信息访问者密钥属性集; $\bar{D}_0$ 表示解密属性集; D_i 表示全部属性集。信息访问者通过区块链平台中发布的密文以及信息拥有者的密文构建安全访问密钥属性集。 T_u 中不包含全部属性集, 因此针对信息访问者进行安全控制

时, 需要求得更多的 T_u , 构建隐私密钥, 以提高网络信息的保护能力。

2 网络信息安全访问控制实现

在进行了对区块链平台、信息拥有者以及信息访问者的参数准备后, 成功获得了不同区块链信息的访问特征和访问权限。基于这些关键信息, 本文特别强调了针对多区块链信息访问场景时, 基于共识点身份信息验证的重要性。通过精确提取并严格验证多区块链间的共识点身份信息, 能够确保每个访问请求的有效性和安全性。每当有新的访问请求产生时, 系统都会生成新的区块并将其添加到原始区块链中, 以进行更进一步的访问控制验证, 从而保障整个信息交换过程的安全性和可靠性。安全访问控制具体实现步骤如下。

在用户注册阶段^[15], 用户访问需要向授权中心发送申请, 在得到申请认证后, 根据其身份编号给出密钥, 然后根据身份编号在属性中心对访问者的身份进行核对, 并将私有密钥转换为公有密钥。

输入用户身份 u_i , 在信息访问者集合中查找与用户身份相关的属性值, 密钥转换身份核对表达式为:

$$S_{u_i} = (B_{1,i} = l_1 h_{u_i}, B_{2,i} = l_2 h_{u_i}, \dots, B_{x,i} = l_x h_{u_i} \mid x \in S) \quad (4)$$

$$K_{u_i} = (K_{1,i} = B_{1,i} R_{sk}, K_{2,i} = B_{2,i} R_{sk}, \dots, K_{x,i} = B_{x,i} R_{sk} \mid x \in S) \quad (5)$$

式中: $B_{x,i}$ 表示用户属性标签; $l_1, l_2, \dots, l_x$ 表示访问序列; h_{u_i} 表示用户身份参数; S 表示属性集合; x 表示用户信息; K_{u_i} 表示与用户属性相对应的转换私有密钥; R_{sk} 表示用户身份密钥。

在信息授权阶段, 信息拥有者需要对被访问信息进行加密并储存在本地数据库中, 设置访问策略并对存储地址进行加密解密。设置 IP 地址函数为 $\zeta(x)$, 生成访问地址控制解密方程为:

$$W = (B_{x,i} \times \zeta(W_{1,x} + W_{2,x} + W_{3,x})) \quad (6)$$

式中: $W_{1,x}$ 表示标签地址的访问控制密钥; $W_{2,x}$ 表示属性地址的访问控制密钥; $W_{3,x}$ 表示关键词地址的访问控制密钥。

针对多区块链间的访问, 需以共识点为基础, 确保数据一致性和安全性。共识点身份信息是建立信任的关键, 包括区块链唯一标识符、共识算法详情和节点列表。提取并验证这些信息, 能确保区块链的真实可靠性。验证过程需严谨, 包括信息完整性核对和安全哈希值比对。验证通过后, 可建立安全通道, 实现跨链数据传输和操作。新访问请求产生时, 系统将生成新区块并加入原始链中, 包含访问摘要和存储地址。基于这些信息, 系统将进行访问控制验证, 确保访问的安全性和合规性。多区块链架构如图 1 所示。

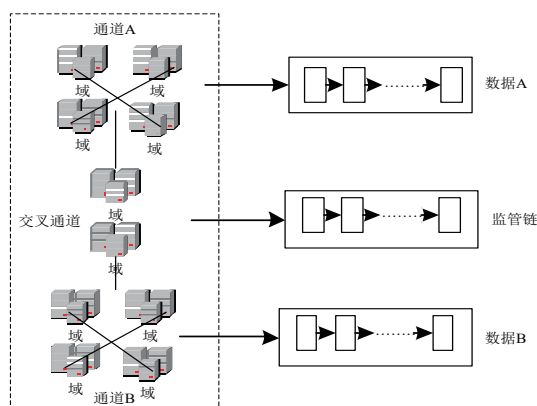


图 1 多链架构示意图

安全访问控制流程如图 2 所示。

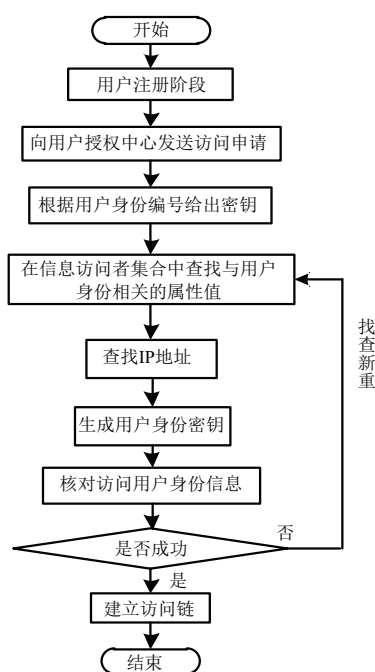


图 2 网络信息安全访问控制流程

3 实验验证分析

3.1 实验环境

实验样本与参数信息如表 1 所示。

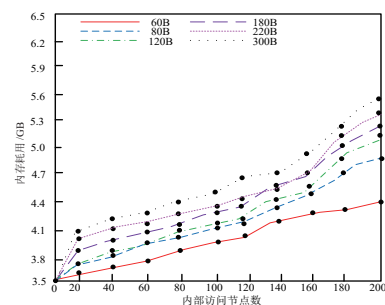
表 1 实验样本和硬件参数

名称	参数 / 特征
开发语言	Java
下载文件最低速率	100 ms
访问节点数量	200 个
系统	Ubuntu 16.04 LTS
吞吐量	50 bit/s
区块链数量	500
文件属性数量	0~2000
溯源地址	初始端 IP
抗攻击性	强

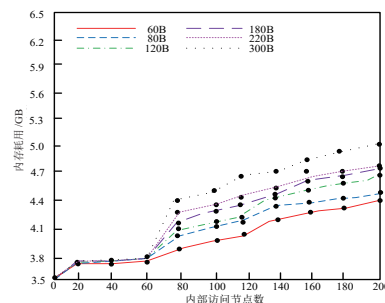
为验证文中提出的基于区块链技术的网络信息安全访问控制方法的有效性，进行实验验证。网络信息中涉及的用户种类较多、信息庞大可满足实验测试条件，访问文件的大小选择为 60 B、80 B、120 B、180 B、220 B 以及 300 B。

3.2 内存耗用结果对比分析

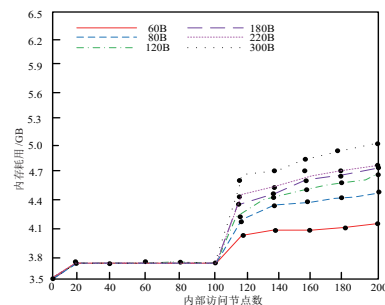
网络信息之间的差异性、种类较多，安全访问控制树的结构会根据信息种类变化而越来越复杂，增加信息拥有者的加密负担。因此，实验将针对不同大小的访问信息，测试不同控制方法运行所产生的空间占用。与策略隐藏大数据访问控制、域间访问控制模型进行对比分析，得到实验对比结果如图 3 所示。



(a) 策略隐藏大数据方法访问控制的内存耗用



(b) 域间访问控制模型访问控制的内存耗用



(c) 所提方法访问控制的内存耗用

图 3 不同控制方法的运行内存耗用对比结果

从图 3 的展示可以看出，3 种不同方法对于内存耗用的结果存在显著差异。其中，所提出的方法在内存耗用方面表现最优，其内存耗用明显低于其他两种方法。这一结果充分证明了所提访问控制方法在实际应用中的有效性。该方法之所以能够实现较低的内存耗用，关键在于它无需进行二次或

多次验证,从而避免了不必要的系统运行空间浪费。在传统的访问控制机制中,为了确保数据的安全性和完整性,可能需要对用户进行多次的身份验证和权限检查,这无疑增加了系统的运行负担和内存耗用。而所提方法通过精准地提取和验证多区块链间的共识点身份信息,实现了高效的访问控制,从而显著降低了内存耗用。

3.3 控制误差结果对比分析

对于多区块链信息间的访问控制,控制误差是评估不同方法性能的关键指标之一。该指标能够量化实际访问控制结果与期望结果之间的差异。当控制误差较小时,意味着该方法在验证用户身份和授权方面具有较高的准确性和可靠性,从而有效保障了多区块链信息的安全性和合规性。测试三种方法的控制误差,得到实验对比曲线如图4所示。

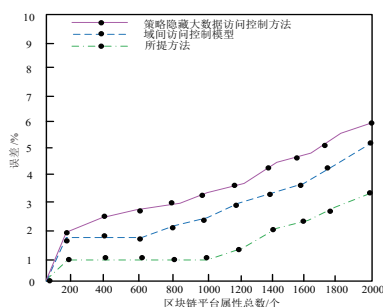


图4 三种方法访问控制误差对比曲线

从图4中可以看出,随着访问验证数据量的不断增长,3种网络信息安全访问控制方法的误差都呈现出一定程度的上升趋势。相比之下,所提方法的误差上升幅度明显小于其他两种方法,这充分说明了该方法在保障多区块链网络信息安全方面的有效性。这一结果不仅证明了所提方法具有较高的实用价值,也展示了其在处理多区块链数据访问验证时的稳定性和可靠性。所提方法的优势在于访问控制和验证机制的设计。通过提取和验证多区块链间的共识点身份信息,实现了对访问请求的精准控制,从而降低了误报和漏报的可能性。这一步骤直接决定了访问控制的准确性和效率。

4 结论

针对跨链信息访问控制的挑战,本方法通过提取和验证多区块链间的共识点身份信息,有效确保了访问请求的有效性和安全性,从而弥补了传统访问控制方法在处理跨链信息时的不足。这种信息验证机制能够预先识别和匹配访问者和被访问者之间的关联信息,并据此计算出匹配的密钥值,为后续的访问控制提供了精确可靠的指令依据。考虑到网络信息复杂多变,本方法通过多个步骤的关联和验证,确保了整个访问过程的逻辑性和安全性。实验结果表明,所提访问控制方法不仅在内存耗用和误差控制方面表现出色,而且在实际应用中展现出较强的性能,为网络信息安全提供了强有力的保障。

参考文献:

- [1] 林莉,储振兴,刘子萌,等.基于区块链的策略隐藏大数据访问控制方法[J].自动化学报,2023,49(5):1031-1049.
- [2] 张建标,张兆乾,徐万山,等.一种基于区块链的域间访问控制模型[J].软件学报,2021,32(5):1547-1564.
- [3] 张亚兵,王健,邢宾.工业互联网中增强安全的云存储数据访问控制方案[J].计算机应用研究,2021,38(12):3765-3770.
- [4] 王杰昌,张平,常琳林,等.可证明安全的用户云数据访问控制协议[J].计算机工程与设计,2022,43(6):1527-1533.
- [5] 罗鸿轩,金鑫,钱斌,等.基于区块链的台区智能终端与智能电表安全防护方法[J].南方电网技术,2021,15(4):50-58.
- [6] 刘雪娇,殷一丹,陈蔚,等.基于区块链的车联网数据安全共享方案[J].浙江大学学报(工学版),2021,55(5):957-965.
- [7] 曾辉祥,习宁,谢晴晴,等.抗属性篡改的去中心化密文数据安全共享[J].西安电子科技大学学报,2022,49(2):135-145.
- [8] 王高洲,王惠剑,王聪,等.基于SM2密码算法的电力数据安全接入方法[J].南京理工大学学报,2022,46(6):749-755.
- [9] 吴万青,赵永新,王巧,等.一种满足差分隐私的轨迹数据安全存储和发布方法[J].计算机研究与发展,2021,58(11):2430-2443.
- [10] 冯涛,陈李秋,方君丽,等.基于本地化差分隐私和属性基可搜索加密的区块链数据共享方案[J].通信学报,2023,44(5):224-233.
- [11] 彭柳,张森,高杰欣.基于区块链技术的电子档案安全存储与可信验证方案[J].中南民族大学学报(自然科学版),2022,41(6):728-733.
- [12] 孙僖泽,周福才,李宇溪,等.基于可搜索加密机制的数据库加密方案[J].计算机学报,2021,44(4):806-819.
- [13] 李满礼,倪明,颜云松,等.面向恶意攻击的安全稳定控制系统信息物理协调防御方法[J].电力系统自动化,2021,45(18):113-121.
- [14] 赖业宁,封科,于同伟,等.基于DHT和区块链技术的电网安全稳定控制终端分布式认证[J].中国电力,2022,55(4):44-53.
- [15] 刘玉红,杨亮,朴春慧,等.基于区块链的铁路工程施工安全监测数据共享关键技术研究[J].通信学报,2021,42(8):206-216.

【作者简介】

张铠(1984—),男,重庆人,硕士,讲师,研究方向:物联网应用技术。

(收稿日期:2024-06-06)