



研究与开发

基于区块链的多源网络大数据安全 访问权限认证仿真

李斌, 何辉, 赵中英, 郭景维

(国网宁夏电力有限公司信息通信公司, 宁夏 银川 750004)

摘 要: 多源网络大数据的频繁交互与存储打破了传统数据“孤岛”, 实现了跨区域与跨组织的数据访问, 为数据的安全和隐私保护带来巨大挑战。访问认证作为保护数据与资源安全的技术之一, 在获取所有数据节点信任的同时, 面临巨大的通信负载, 会造成数据丢失和破坏, 为此, 提出一种基于区块链研究多源网络大数据安全访问权限认证方法。以相似关系度量数据在网络传输中的变化状态, 根据相似矩阵计算多源网络数据访问概率。通过区块链技术建立数据安全访问合约, 标定数据的访问属性以及交易密文, 并将数据压缩在对应属性内。根据访问目的分析其访问信度, 以信度作为标准对应安全等级, 在不同信度下定制访问规则, 认证数据安全访问的具体权限, 实现方法设计。实验结果表明, 以不同数据属性含量作为测试条件, 在常规模式和攻击模式下对数据进行加密和解密处理, 新方法可以实现较快的认证响应, 实现网络数据的安全访问。

关键词: 区块链; 多源网络; 大数据; 安全访问; 权限认证

中图分类号: TP393

文献标志码: A

doi: 10.11959/j.issn.1000-0801.2024021

Security access permission authentication simulation of multi-source network big data based on blockchain

LI Bin, HE Hui, ZHAO Zhongying, GUO Jingwei

State Grid Ningxia Electric Power Company, Yinchuan 750004, China

Abstract: The frequent interaction and storage of big data in multi-source networks have broken traditional data silos, enabling cross regional and cross organizational data access, posing significant challenges to data security and privacy protection. As one of the technologies to protect data and resource security, access authentication faces enormous communication loads while obtaining trust from all data nodes, which can cause data loss and damage. Therefore, a blockchain based research method for multi-source network big data security access permission authentication was proposed. The transformation status of data in network transmission using similarity relationships was measured, and the probability of multi-source network data access based on the similarity matrix was calculated. The data security access contracts were established through blockchain technology, calibrating data access attributes and transaction ciphertexts, and compressing data within corresponding attributes. The access reliability based on the purpose of the

收稿日期: 2023-06-30; 修回日期: 2023-12-30



access was analyzed, reliability was used as the standard to correspond to the security level, rules under different levels of reliability were accessed, specific permissions were authenticated for data security access, and implementation methods were designed. The experimental results show that using different data attribute contents as testing conditions, encrypting and decrypting data in both conventional and attack modes, the new method can achieve fast authentication response and secure access to network data.

Key words: blockchain, multi-source network, big data, secure access, authority authentication

0 引言

信息技术不断地改变着人类的生活方式,人类在互联网中分享生活,这样每天会产生数以万计的数据,如何保证数据传输和应用的安全性,是保证网络运行安全的重要研究课题。文献[1]提出了一个新方法,主要对大规模网络的访问进行控制,采用跨域方式引入信息属性概念,在相似性测量下对数据信息进行自动选择,达到数据评估的目的,在整体应用过程中该方法能够对数据进行有效评估,从而保证网络的访问安全性。文献[2]基于差分隐私技术设计了大数据安全访问权限认证,主要是通过拉普拉斯方式对数据进行统计,从而达到隐私保护的效果。在对数据对象划分的基础上,对数据类型进行标签授权,按照不同的类型进行管理,在实际应用中具有较高的安全性。为实现多角度的数据安全访问权限认证,需要通过多种手段对数据进行访问控制。其中,区块链技术可以在开放的环境下直接建立信任关系,能够实现数据的存储和交换,具有全程透明、全程跟踪以及难以伪造的特征。通过使用区块链技术,可以建立数据安全访问合约,标定数据的访问属性以及交易密文,并将数据压缩在对应属性内。同时,通过分析访问目的信度并设置不同安全等级,可以定制访问规则并认证数据的安全

访问权限。L2 区块链技术是指在第二层上构建的区块链解决方案,它通过与底层区块链网络进行交互,实现了更高的扩展性和效率。相比于传统的智能合约,L2 区块链技术能够提供更快的交易确认速度和更低的交易费用。基于此,本文以区块链技术作为研究基础,对多源网络大数据的安全访问和权限认证进行分析,设计一个新的安全访问权限认证方法,为数据的安全共享提供技术支持。

1 相似关系计算多源网络数据访问概率

大数据在多源网络传输中会经历多次传播,而在不同的用户标注下会呈现出不同的访问安全性,为保证多源网络的运行安全,需要对大数据的访问权限进行认证。而数据类型的数据传输存在关联性,以相似关系进行计算,能够度量数据传输前后的状态,基本思想为:

$$\begin{cases} U \leftrightarrow I \\ T \leftrightarrow Y \leftrightarrow U \leftrightarrow I \\ T \leftrightarrow Y \end{cases} \quad (1)$$

其中,随机选择4组数据对象,分别为 T 、 Y 、 U 、 I 。“ $\leftrightarrow$ ”为相似关系^[3]，“ $\Leftrightarrow$ ”为关联条件。式(1)表示:当 U 、 I 具有相似性, T 、 Y 又能够与 U 、 I 关联,则 T 、 Y 也具有相似性。通过数据对象之间的关系,对相似度进行计算:

$$O(T, Y) = \begin{cases} 1, & T = Y \\ \frac{P}{|A(T)||A(Y)|} \sum_T \sum_T O(A_T(T), A_Y(T)), & T \neq Y \cap A(T), A(Y) \neq \emptyset \\ 0, & \text{其他} \end{cases} \quad (2)$$

$$O(U, I) = \begin{cases} 1, & U = I \\ \frac{P}{|S(U)||S(I)|} \sum_T \sum_T^{S(U)||S(I)|} O(S_U(U), S_I(I)), & U \neq I \cap S(U), S(I) \neq \emptyset \\ 0, & \text{其他} \end{cases} \quad (3)$$

其中, $S(U)$ 、 $S(I)$ 为输出状态。 $A(T)$ 、 $A(Y)$ 为输入状态。 $O(T, Y)$ 、 $O(U, I)$ 为相似度。 P 为常量衰减因子。假定数据对象具有相似性, 通过相似度建立相似度矩阵, 如下:

$$\mathbf{F}(U, I) = \begin{cases} 0, U \neq I \\ 1, U = I \end{cases} \quad (4)$$

$$\mathbf{F}(T, Y) = \begin{cases} 0, T \neq Y \\ 1, T = Y \end{cases} \quad (5)$$

其中, $\mathbf{F}(U, I)$ 为 U 、 I 的相似度矩阵^[4]。 $\mathbf{F}(T, Y)$ 为 T 、 Y 的相似度矩阵。通过上述数据的举例, 在大量数据传输过程中, 以同类型数据为并行计算标准, 获取数据的访问概率:

$$\mathbf{G}^K = P * \mathbf{F}(U, I) + (1 - P) * \mathbf{F}(T, Y) \quad (6)$$

其中, $\mathbf{G}^K$ 为访问概率^[5-7]。由于多源网络的数据传输量较大, 直接对其访问概率进行计算会有较大的难度, 因此采用相似度作为划分基础, 对数据在网络中的访问概率进行计算, 并通过计算结果设定数据的访问合约。通过考虑数据的相似关系和使用区块链建立合约, 能够更精确地确定数据的访问权限, 避免未经授权的数据访问和减少数据泄露的风险。

2 基于区块链技术生成数据安全访问合约

通过计算得到的数据历史访问概率, 能够看出多源网络数据在访问中会形成独立的数据孤岛, 为实现数据的安全交换和应用, 采用区块链技术生成数据的安全访问合约。区块链技术能够将分散的数据与其相应属性对应起来, 确保数据在传输和存储过程中的安全性和难以篡改性, 从而提高数据的整体安全保障水平。一般情况下每个数据会对应一个访问合约, 过程如下:

$$U = I$$

其他

$$d_\beta = \text{details}\{(f_\beta)\} \quad (7)$$

其中, $\text{details}(\cdot)$ 为区块链技术中的合约函数。 d_β 为区块链事务散列, 表示为 $d_\beta = \{d_1, d_2, \dots, d_\chi\}$ ^[8-10]。

f_β 为等待交换的数据, 即 $f_\beta = \{f_1, f_2, \dots, f_\chi\}$, 其中 χ 为总数。通过合约函数能够在网络中建立一个公开协议, 一旦合约部署成功, 数据对应在其属性策略之内, 并通过区块链的签名属性辅助数据访问。

基于区块链技术能够将数据的安全访问划分为 3 个步骤, 分别为初始化数据、数据注册、数据访问控制。对于不同的步骤均需要一个合法的区块链数据账户, 在初始化中包括密钥生成和事务绑定, 如下:

$$\{gh_j, kh_j\} = \text{rsa}(k_1, k_2) \quad (8)$$

$$d_\beta'' = (lh_j, x(\delta)) \quad (9)$$

其中, lh_j 为加密属性的公钥, h_j 为 rsa 属性密钥, $\{gh_j, kh_j\}$ 为密钥对, k_1 、 k_2 为随机素数, d_β'' 为放置在区块链中的事务。

在对数据初始化加密之后, 需要对数据的访问进行注册, 根据访问策略决定数据的访问属性, 并在注册后对数据进行分配, 通过区块链生成交易访问的密文。注册过程包括交易标识、访问摘要以及密文, 如下:

$$\text{cd} = (lh_b(v_1, v_2, \dots, v_\chi)) \quad (10)$$

$$n = \text{hash}(m) \quad (11)$$

$$\begin{cases} Q = (n, \text{ass}^*, \text{cd}) \\ \text{token} = (\text{sign}(\text{cd}, \text{ass}^*, \epsilon)) \end{cases} \quad (12)$$

其中, cd 为密文, lh_b 为在区块链读取的公钥, 并且 $b \neq j$ ^[11-15], $(v_1, v_2, \dots, v_\chi)$ 为对应属性集合, n 为



访问摘要, $\text{hash}(\cdot)$ 为散列函数, m 为数据内容, Q 为交易标识, ass^* 为唯一访问地址, $\text{sign}(\cdot)$ 为执行函数^[16-19], ε 为子账户密钥, token 为返回令牌。

在数据属性注册后对其进行验证, 根据区块链中的访问策略进行压缩组合, 生成对应的数据安全访问权限合约, 具体如下:

$$\{\text{rull}_1, \text{rull}_2, \dots, \text{rull}_x\} = W(\gamma^{-1} \times x(\delta)) \quad (13)$$

其中, $[\text{rull}]$ 为生成合约。 γ^{-1} 为压缩操作^[20-22]。 $W(\cdot)$ 为分布函数。在每一个数据属性中均可以在压缩后, 通过区块链技术生成访问合约, 并根据合约的具体内容计算数据的安全等级, 从而认证数据的安全访问权限。

3 安全等级定制规则认证数据安全访问权限

根据追溯到的数据安全访问目的, 将网络中的数据对应所属的两个位置, 并根据数据访问的安全等级制定相应规则, 实现对网络大数据的安全访问权限认证。数据的安全等级可以表示多源网络中用户的状态, 因此用户的可信度是衡量数据安全等级的基础, 以计分换算的方式来描述用户状态:

$$\begin{aligned} q &= \{q_1, q_2, \dots\} \\ e &= \{e_1, e_2, \dots\} \end{aligned} \quad (14)$$

其中, q 为用户数据集合, e 为信度权重。为了体现数据的安全性, 直接通过信度权重表示访问的重要程度, 当 e 越大时表示信息的安全性越重要。基于此, 对多源网络中的数据信息给予重要程度, 多源网络数据安全访问程度值见表 1^[23]。

表 1 多源网络数据安全访问程度值

数值	含有
1	数据的安全性同样重要
3	前一组数据比后一组的安全性稍微重要
5	前一组比后一组的重要
7	前一组的安全性比后一组更重要
9	相比后一组数据, 前一组安全性非常重要
2/4/6/8	重要程度在中间位置
倒数	相反含义

根据表 1, 在求取数据的安全等级过程中, 数据的权重是一个重要的指标, 为获取数据的权重值, 需要将数据随机选择两组相邻访问的网络数据, 对其安全性的重要程度进行比较, 并将得到的结果进行归一化处理。计算式如下:

$$e_w = \frac{\sum_{t=1}^r u_{wt}}{\sum_{t=1}^r \sum_{w=1}^r u_{wt}} \quad (15)$$

其中, e_w 为权重矩阵^[24]。 u_{wt} 为比较矩阵, 表示为 $(u_{wt})_{r \times r} = u$ 。 w 、 t 为信息标号, 其中 $w \in r$ 、

$t \in r$, 且 $u_{wt} > 0$ 、 $u_{wt} = \frac{1}{u_{tw}}$ 、 $u_{ww} = 1$ ^[25]。在

源网络中对数据进行安全访问权限认证, 可以直接通过信度换算制定规则, 信度计算式为:

$$i_w = \frac{o_w}{p_w} \quad (16)$$

其中, i 为信度等级比例值, 其取值范围为 $i \in [0, 1]$, 可以直接表示信息的可信性^[26]。 o 为数据单项评分。 p 为单项分值, 取值为 $p = 10$ 。根据式 (16) 求取信息数据在网络中的可信度比例, 建立判断标准, 安全访问信度比例判断标准见表 2。

表 2 安全访问信度比例判断标准

数据	等级标准
a1	>2 次
	=2 次
	=1 次
	=0 次
a2	当前发生变化
	无变化, 但有历史记录
a3	无变化
	>2 次
	=2 次
	=1 次
	=0 次

根据表 2, $a1$ 为非法操作数据, $a2$ 为数据的终端位置, $a3$ 为验证失败次数。将其构建为信度

比例集合, 为 $a = \{a_1, a_2, a_3\}^{[27]}$ 。以信度比例与数据权重相结合, 反映数据的安全等级, 如下:

$$s = e * a = [e_1 \quad e_2 \quad e_3] * \begin{bmatrix} a_1 \\ a_2 \\ a_3 \end{bmatrix} \quad (17)$$

其中, s 为数据的可信度, 即访问的安全等级。通过计算的数据重要程度, 将其对应应在响应的等级集合之内, 判断数据是否能够在多源网络中进行访问, 得到授权后根据不同的等级设定访问顺序。

根据用户的访问信度和安全等级, 可以为每个用户提供个性化的访问权限认证, 确保数据访问在授权范围内进行, 并提供更灵活的访问控制方案。至此, 本文基于区块链技术实现多源网络大数据安全访问权限认证方法设计。

4 实验测试分析

上文通过区块链技术设计了新的认证方法, 为验证新方法可以在多源大数据安全访问过程中实现了有效的权限认证, 以对比测试的方式进行论证。采用跨域认证方法和基于差分隐私的认证方法作为对照组, 分别与本文方法进行对比, 以验证不同方法的有效性。

4.1 搭建测试环境

为保证此次测试的真实性, 需要将选择的 3 组认证方法放置在统一的环境中, 分别对各组方法的加密以及解密情况进行验证。选择多源互联网作为测试对象, 对其访问用户产生的数据进行访问认证, 当用户进入网络系统时, 该用户有权利发起新的数据访问, 因此需要通过认证方法进行权限管理和控制。基于此, 搭建此次测试环境, 详情见表 3。

由表 3 可知, 设计此次网络系统中的数据访问功能, 包括历史数据查询以及新数据的生成和管理, 当用户进入到网络系统时, 可以对历史数据进行查询, 也可以发出新的数据访问请求。通过搭建的测试系统连接 3 组安全访问权限认证方

法, 对网络系统的数据进行访问权限管理, 以验证不同方法下的响应时间。

表 3 测试环境详情

内容	参数
操作系统	Ubuntu18.05-128 bit
开发工具	Eclipse JUNO25.0.2 Android Studio4.2.2 Sublimetext5 MySQL Workbench5.2.6
内存	Intel (R) Core (RM) I10-2 800 K
CPU	64.0 GB

4.2 验证各组认证方法响应时间

在用户通过网络端发送数据交易时, 各组方法会产生相应的调试码, 通过调试码在网络中进行连接, 并向用户传回相应的数据结果。为此, 在进行各组方法的安全访问权限认证前, 需要针对不同方法的响应时间进行测试, 将响应时间作为判断标准, 只有能够对大量的数据实现快速响应, 才能保证密钥的快速生成。分别以常规模式和带有威胁因素的模式作为测试前提, 验证各组认证方法的响应时间, 不同数据量下权限认证响应时间如图 1 所示。

图 1 中, 以数据中的属性个数作为变化条件, 随着时间的增加, 数据中的属性会不断增加, 当数据量发生变化时各组认证方法的响应时间会发生变化。无论是哪一种模式, 本文方法可以一直保持在 20~30 ms 范围, 两组传统方法的响应时间, 在常规模式下最终超过 400 ms, 而威胁攻击下最终超过 700 ms, 说明本文方法更适用于多源网络的大数据访问控制。这是因为本文方法引入了区块链技术建立数据安全访问合约, 区块链的去中心化特性可以提高系统的性能和响应速度。

4.3 测试数据加密与解密响应效率

上文验证了各组方法的响应时间, 在此基础上验证各组方法的加密和解密时间, 在数据安全访问权限认证过程中, 只有对数据进行加密才能实现对其的有效控制, 并在传输完毕后对数据进

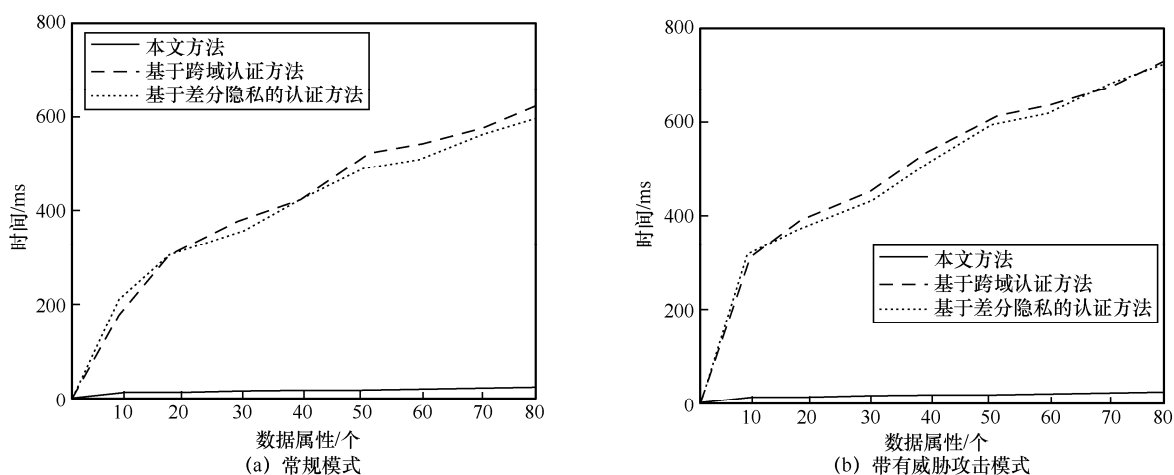


图1 不同数据量下权限认证响应时间

行解密,按阶段完成上述两个步骤,才是对数据的安全访问权限整体认证。以上文中的两种模式作为测试条件,分别验证不同认证方法的加密和解密响应时间,其中,常规模式下的验证结果如图2所示。

图2中,在本文方法应用下对数据的加密和解密均可以保证在40 ms以内,且加密时间与解密时间差异性较小,而两组传统方法的响应时间超过500 ms,主要是其对数据的响应时间较长。

在完成常规模式的响应测试后,在网络中加

入威胁攻击,分别测试不同方法的加密和解密时间,攻击模式下的测试结果如图3所示。

图3中,当发生网络攻击时,传统方法的响应时间接近2 000 ms,且加密和解密的响应时间的差异性较大,但本文方法的加密和解密时间,仍能保证在60 ms以内,且两者没有产生较大差异。这是因为本文综合两种测试结果,均可以说明本文方法不仅在正常模式下表现出较快的响应速度,而且在面对威胁和攻击时仍能保持高效的加密和解密处理能力,从而确保数据的安全访问和保护。

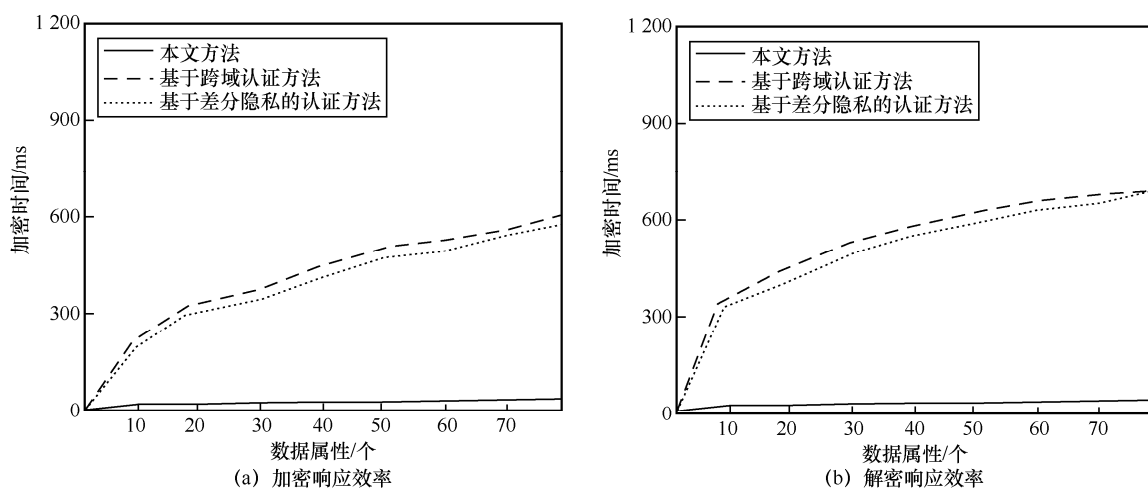


图2 常规模式下的验证结果

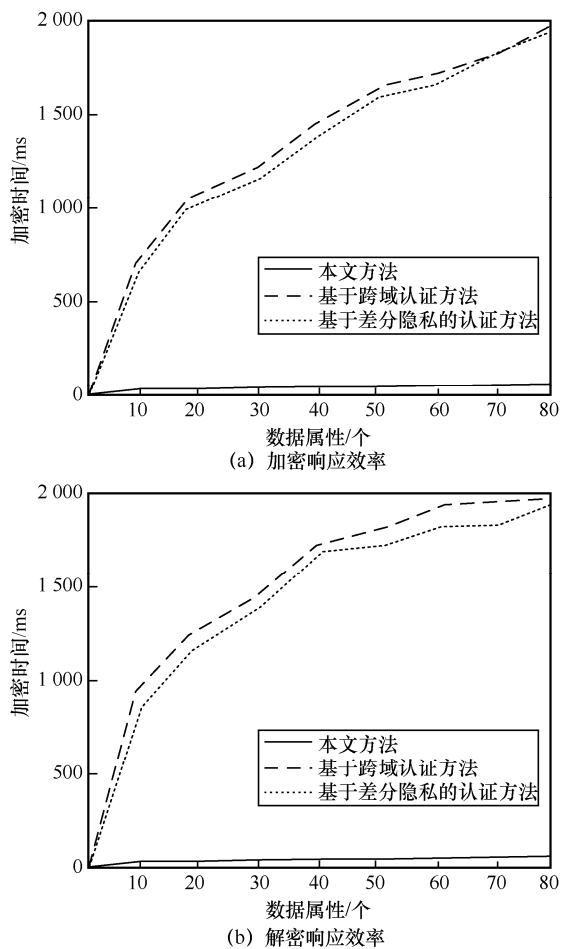


图3 攻击模式下的测试结果

5 结束语

随着物联网和云计算的快速发展,以数据为载体的分布式网络结构形成了,而数据访问呈现跨区域以及跨组织的特点。在大数据时代中,数据的安全访问和服务得到了更多的关注,当数据发生频繁交换以及存储时,会受到威胁因素的攻击,导致数据的表达发生改变,甚至数据的存储结构遭受破坏。为此,本文基于区块链技术设计了新的大数据安全访问权限认证方法,对数据的访问机制进行控制,获取了较好的安全认证效果,具有一定的应用价值。

参考文献:

[1] 唐坤剑,冯光辉.大规模网络跨域云安全访问控制方法仿

真[J]. 计算机仿真, 2023, 40(2): 434-437, 529.

TANG K J, FENG G H. Simulation of cross domain cloud security access control methods for large-scale networks[J]. Computer Simulation, 2023, 40(2): 434-437, 529.

[2] 刘东,任海玲.基于差分隐私的大数据安全访问权限认证仿真[J]. 计算机仿真, 2021, 38(8): 421-424, 486.

LIU D, REN H L. Big data security access authentication simulation based on differential privacy[J]. Computer Simulation, 2021, 38(8): 421-424, 486.

[3] 郑荣,高志豪,魏明珠,等.基于联盟区块链的政府数据协同治理平台框架研究:以全国碳排放权交易市场为例[J]. 情报学报, 2022, 41(10): 1071-1084.

ZHENG R, GAO Z H, WEI M Z, et al. Framework of the government-data collaborative governance platform based on the alliance blockchain: considering the national carbon emissions trading market as an example[J]. Journal of the China Society for Scientific and Technical Information, 2022, 41(10): 1071-1084.

[4] 朱向荣,吴鸿祜,胡伟. FactChain: 一个基于区块链的众包知识融合系统[J]. 软件学报, 2022, 33(10): 3546-3564.

ZHU X R, WU H H, HU W. FactChain: a blockchain-based crowdsourcing knowledge fusion system[J]. Journal of Software, 2022, 33(10): 3546-3564.

[5] 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.

LAI Y N, FENG K, YU T W, et al. Distributed authentication of power grid safety and stability control terminals based on DHT and blockchain[J]. Electric Power, 2022, 55(4): 44-53.

[6] 杨坤伟,杨波,周彦伟.群智网络中基于区块链的有序聚合签名认证方案[J]. 电子学报, 2022, 50(2): 358-365.

YANG K W, YANG B, ZHOU Y W. A sequential aggregate signature authentication scheme based on blockchain for crowdsensing system[J]. Acta Electronica Sinica, 2022, 50(2): 358-365.

[7] 宋涛,李秀华,李辉,等.大数据时代下车联网安全加密认证技术研究综述[J]. 计算机科学, 2022, 49(4): 340-353.

SONG T, LI X H, LI H, et al. Overview of research on security encryption authentication technology of IoV in big data era[J]. Computer Science, 2022, 49(4): 340-353.

[8] 廉文娟,赵朵朵,范修斌,等.基于认证及区块链的CFL BLP_BC模型[J]. 计算机科学, 2021, 48(11): 36-45.

LIAN W J, ZHAO D D, FAN X B, et al. CFL BLP BC model



- based on authentication and blockchain[J]. Computer Science, 2021, 48(11): 36-45.
- [9] 张利华, 张赣哲, 曹宇, 等. 基于区块链的智能家居认证与访问控制方案[J]. 计算机应用研究, 2022, 39(3): 863-867, 873.
- ZHANG L H, ZHANG G Z, CAO Y, et al. Authentication and access control scheme for smart home based on blockchain[J]. Application Research of Computers, 2022, 39(3): 863-867, 873.
- [10] 耿文莉, 高梦瑜. 基于灰色神经网络的云平台大数据安全风险评估[J]. 科学技术与工程, 2021, 21(28): 11932-11937.
- GENG W L, GAO M Y. Security risk assessment of big data on cloud platform based on grey neural network[J]. Science Technology and Engineering, 2021, 21(28): 11932-11937.
- [11] 张山山. 基于区块链的舰船航行大数据共享安全认证研究[J]. 舰船科学技术, 2021, 43(18): 82-84.
- ZHANG S S. Research on security authentication of ship navigation big data sharing based on blockchain[J]. Ship Science and Technology, 2021, 43(18): 82-84.
- [12] 彭红艳, 李杰, 石贞奎, 等. 一种基于区块链可验证的加密图像检索方案[J]. 计算机工程, 2022, 48(2): 25-33, 39.
- PENG H Y, LI J, SHI Z K, et al. A blockchain-based verifiable encrypted image retrieval scheme[J]. Computer Engineering, 2022, 48(2): 25-33, 39.
- [13] 黄更生, 黄宇红, 郭漫雪, 等. DT 时代面向数据服务的新型基础设施架构[J]. 电信科学, 2022, 38(7): 138-145.
- HUANG G S, HUANG Y H, GUO M X, et al. Architecture of a new infrastructure for data service in DT era[J]. Telecommunications Science, 2022, 38(7): 138-145.
- [14] 李养群, 张登银. 物品万维网资源管理框架研究与应用[J]. 物联网学报, 2022, 6(2): 50-64.
- LI Y Q, ZHANG D Y. Research and application of Web of things resource management framework[J]. Chinese Journal on Internet of Things, 2022, 6(2): 50-64.
- [15] 晏燕, 丛一鸣, MAHMOOD A, 等. 基于深度学习的位置大数据统计发布与隐私保护方法[J]. 通信学报, 2022, 43(1): 203-216.
- YAN Y, CONG Y M, MAHMOOD A, et al. Statistics release and privacy protection method of location big data based on deep learning[J]. Journal on Communications, 2022, 43(1): 203-216.
- [16] 林楠, 吴林峰, 方洪波. 大数据环境下电力网络数据安全入侵模型仿真[J]. 现代电子技术, 2022, 45(4): 118-122.
- LIN N, WU L F, FANG H B. Simulation of intrusion model for power network data security in big data environment[J]. Modern Electronics Technique, 2022, 45(4): 118-122.
- [17] 牛淑芬, 方丽芝, 宋蜜, 等. 智慧城市中隐私保护性广播加密算法[J]. 计算机工程与科学, 2022, 44(6): 1003-1012.
- NIU S F, FANG L Z, SONG M, et al. Privacy-preserving broadcast encryption in smart city[J]. Computer Engineering & Science, 2022, 44(6): 1003-1012.
- [18] 曾智勇, 洪睿, 李祥林. 物联网下差异设备兼容数据安全访问控制模型研究[J]. 自动化仪表, 2022, 43(8): 112-117.
- ZENG Z Y, HONG R, LI X L. Research on disparate device compatible data security access control model under IoT[J]. Process Automation Instrumentation, 2022, 43(8): 112-117.
- [19] 谭继安. 基于决策树和混合神经网络的大数据攻击增量检测研究[J]. 计算机应用与软件, 2022, 39(7): 329-335, 349.
- TAN J A. Incremental detection for big data attacks based on decision tree and hybrid neural network[J]. Computer Applications and Software, 2022, 39(7): 329-335, 349.
- [20] 刘龙庚. 基于异构网络空管安全监控关联算法研究[J]. 信息网络安全, 2022(4): 58-66.
- LIU L G. Research on association algorithm of heterogeneous network security monitoring[J]. Netinfo Security, 2022(4): 58-66.
- [21] 殷昱煜, 叶炳跃, 梁婷婷, 等. 边缘计算场景下的多层区块链网络模型研究[J]. 计算机学报, 2022, 45(1): 115-134.
- YIN Y Y, YE B Y, LIANG T T, et al. Research on multi-layer blockchain network model in edge computing[J]. Chinese Journal of Computers, 2022, 45(1): 115-134.
- [22] 王育齐, 陈庚, 钱伟中. 区块链环境下用户身份匿名的量子委托计算协议[J]. 电子科技大学学报, 2022, 51(6): 802-811.
- WANG Y Q, CHEN G, QIAN W Z. Quantum delegate computing protocol with anonymous user identity in blockchain scenario[J]. Journal of University of Electronic Science and Technology of China, 2022, 51(6): 802-811.
- [23] 黄晓舸, 刘鑫, 何勇, 等. 基于区块链的雾网络中的任务卸载优化方案研究[J]. 电子与信息学报, 2022, 44(7): 2440-2448.
- HUANG X G, LIU X, HE Y, et al. Research on optimization scheme of task offloading in blockchain-enabled fog networks[J]. Journal of Electronics & Information Technology, 2022, 44(7): 2440-2448.
- [24] 钟运琴, 朱月琴, 焦守涛. 边缘大数据分析预测建模方法研究[J]. 高技术通讯, 2022, 32(10): 1067-1075.
- ZHONG Y Q, ZHU Y Q, JIAO S T. Research on edge big data

- analysis and predictive modeling method[J]. Chinese High Technology Letters, 2022, 32(10): 1067-1075.
- [25] 杨昌霖, 王继光, 汪清. 无线物联网中局部有向无环图区块链研究[J]. 计算机应用研究, 2022, 39(9): 2597-2602.
- YANG C L, WANG J G, WANG Q. Local directed acyclic graph blockchain in wireless Internet of Things[J]. Application Research of Computers, 2022, 39(9): 2597-2602.
- [26] 李娜, 周瑛, 曹丽娜. 串口服务器内外网数据安全通信方法仿真[J]. 计算机仿真, 2022, 39(7): 208-212.
- LI N, ZHOU Y, CAO L N. Simulation of secure data communication method between internal and external network of serial port server[J]. Computer Simulation, 2022, 39(7): 208-212.
- [27] 姚云霞, 张国权. 区块链数据防篡改备份恢复算法与仿真[J]. 计算机仿真, 2022, 39(11): 411-415.
- YAO Y X, ZHANG G Q. Algorithm and simulation for blockchain data tamper-proof backup and recovery[J]. Computer Simulation, 2022, 39(11): 411-415.

[作者简介]



李斌(1985-), 男, 国网宁夏电力有限公司信息通信公司高级工程师, 主要研究方向为大数据技术、人工智能技术、电力信息系统智能化运维及网络安全等。

何辉(1995-), 男, 国网宁夏电力有限公司信息通信公司助理工程师, 主要研究方向为电力信息安全。

赵中英(1990-), 男, 国网宁夏电力有限公司信息通信公司工程师, 主要研究方向为信息系统运维技术、数据运营管理和数据安全等。

郭景维(1984-), 男, 国网宁夏电力有限公司信息通信公司高级工程师, 主要研究方向为电力信息技术等。