

应用轻量级双向认证协议的公共数据安全优化算法

张悦¹, 周鑫²

(1. 中国人民公安大学 涉外警务学院, 北京 100089; 2. 国防科技大学 信息通信学院, 武汉 430000)

摘要: 针对公共数据来源广、信息量大、敏感性高且单向身份认证网络易遭受多种攻击, 导致公共数据安全性不足的问题, 提出了一种应用轻量级双向认证协议的公共数据安全优化算法。该算法结合物理不可克隆函数(PUF)和同步化随机数, 获得轻量级双向认证协议, 降低优化过程中的运算和通信开销。通过可信网络连接对协议接入过程中用户读写器的可信度进行认证, 将同步化随机数设置于用户读写器与公共数据电子标签两端, 并将 PUF 融入公共数据电子标签内, 增强海量公共数据电子标签密钥对各类攻击的抵抗性能, 完成用户读写器与公共数据电子标签的双向身份认证, 实现敏感数据的安全优化防护。研究表明, 该算法可有效抵抗公共数据存储和传输过程中的去同步化攻击、克隆攻击、中间人攻击等 10 种攻击, 且具有较低的时延, 可保障公共数据的安全性。

关键词: 轻量级; 双向认证协议; 公共数据; 安全优化; 不可克隆函数; 同步化随机数

中图分类号: TP393 **文献标志码:** A **文章编号:** 1671-5497(2026)03-0772-07

DOI: 10.13229/j.cnki.jdxbgxb.20241032

Public data security optimization algorithm using lightweight bidirectional authentication protocol

ZHANG Yue¹, ZHOU Xin²

(1. School of International Policing, People's Public Security University of China, Beijing 100089, China; 2. College of Information and Communication, National University of Defense Technology, Wuhan 430000, China)

Abstract: To address the problem of insufficient security of public data caused by its characteristics of wide sources, large information volume, and high sensitivity, as well as the vulnerability of one-way authentication networks to various attacks, an optimized public data security algorithm applying a lightweight mutual authentication protocol was proposed. A lightweight mutual authentication protocol was obtained by combining Physical Unclonable Functions (PUF) with synchronized random numbers in this algorithm, which reduces the computational and communication overheads during the optimization process. The credibility of user readers during protocol access was authenticated through trusted network connections. Synchronized random numbers were deployed at both ends of user readers and public data electronic tags, and PUF was integrated into the public data electronic tags to enhance the resistance of

收稿日期: 2024-09-23.

基金项目: 国家自然科学基金项目(62201581).

作者简介: 张悦(1996-), 女, 讲师, 博士研究生. 研究方向: 公共安全. E-mail: 13261708806@163.com

keys in massive public data electronic tags against various attacks. Thus, mutual identity authentication between user readers and public data electronic tags was completed, and secure optimized protection of sensitive data was achieved. The research results show that the algorithm can effectively resist 10 types of attacks, including de synchronization attacks, cloning attacks, and man in the middle attacks, during the storage and transmission of public data, and has low latency, which can ensure the security of public data.

Key words: lightweight; bidirectional authentication protocol; public data; safety optimization; unclonable functions; synchronize random numbers

0 引言

公共数据是数据开放主体在依法履职过程中采集和产生、以电子化形式记录和保存的各类数据资源,主要包括社会团体数据、公共企事业单位数据、政务数据、其他社会组织数据等,其特征涵盖多源性、权威性、价值性、敏感性等^[1-3]。根据社会需求和公共利益的导向,需推动公共数据在法律法规允许范围内最大限度地开放利用^[4],同时需确保数据的安全可控,达到明确保护敏感数据、防止数据泄露、确保合规性等总体目标^[5,6]。为此,需采用恰当的方法对公共数据的存储和传输过程实施安全优化保护,确保公共数据免受未授权访问和恶意攻击,提升公共数据的安全性。

目前,已有部分国内外学者针对该领域展开相关研究。例如,吴万青等^[7]提出的数据安全存储和发布方法,以数据时空特征为依据,建立数据轨迹等价类别,结合 Hilbert 曲线划分建立的数据轨迹点,通过聚类所得轨迹中心点得到全新数据轨迹,实现数据空间简化。随后,创建数据前缀树并输入全新数据轨迹,采用等差隐私预算分配法将噪声数据点添加至前缀树中,以提升数据安全性。该方法通过合理的噪声添加和数据扰动处理,在保护隐私的同时,保持了数据的可用性和准确性。但采用等差隐私预算分配法时需要向数据中添加噪声,而噪声的大小和分布计算涉及复杂的数学运算和统计分析,这导致计算复杂度较高、数据处理时间较长,不利于数据安全防护的时效性。赵骏等^[8]提出的物联网数据存储和共享方法,通过创建区块链与 IOTA 双账本,并结合委托权益证明(Delegated proof of stake, DPoS)算法,有效应对物联网数据存储和传输过程中的恶意节点攻击问题,保证数据的安全性。该方法的双账本结构使不同主体间的数据共享变得更加便捷。但双账本结构和区块链技术的引入,使整个方法的运算复杂度显著增加,尤其在针对海量数据的

安全防护时,整体效率不佳。Li等^[9]提出了金融数据安全存储和访问控制方法,通过创建基于属性的访问控制模型,并结合区块链智能合约,实现金融数据的细粒度访问控制。该方法借助区块链技术的分布式账本和加密算法,确保数据的不可篡改性和完整性,但存在隐私泄露的风险,特别是在公共区块链上,交易信息对所有参与者可见,会降低数据整体的安全性。万征等^[10]提出的大健康数据存储和共享模型,以区块联盟链为依据创建双链网络模型,实现大健康数据密文与跨域访问记录的安全存储;同时结合代理重加密算法,重加密数据的跨域记录,保障数据共享的安全性。该模型的区块链共识机制可确保网络节点对数据的正确性达成一致,避免数据冗余和误差,提高数据的一致性和可信度。虽然区块链技术可以提供一定的数据隐私保护,但在数据脱敏不彻底或智能合约设计存在漏洞时,仍可能导致隐私数据泄露。

轻量级双向认证协议是一种在资源受限环境下实现双方安全认证的协议。该协议要求在保证安全性的同时,尽量降低计算复杂度和存储开销,以适应低成本、低功耗的设备,具有双向认证、轻量级、安全性等特点。该协议要求通信双方在交互过程中相互验证身份,保证通信安全性,同时需考虑设备的资源限制,尽量减少计算和存储开销,适配各类轻量化终端。另外,该协议需有效抵抗中间人攻击、重放攻击、密码分析攻击等各种攻击,保证通信数据的机密性、完整性和前向安全性。基于上述研究,本文应用轻量级双向认证协议,设计了一种公共数据安全优化算法,实现对公共数据存储和传输过程中各类攻击的实时、精准安全防护,为公共数据安全提供可靠保障。

1 公共数据安全防护设计

1.1 轻量级双向认证协议下公共数据安全防护

公共数据中包含个人隐私、商业机密等敏感信息,需要采用安全性高的认证机制进行保护。

轻量级双向认证协议通过双向身份认证和密钥协商,可确保通信双方的身份真实性和会话密钥的安全性,有效抵御假冒攻击、中间人攻击等安全威胁。为此,本文应用轻量级双向认证协议^[11]设计公共数据安全防护算法,该算法涉及的关键符号及其定义如表 1 所示。

表 1 算法关键符号及定义

Table 1 Key symbols and definitions of the algorithm

符号	定义
R	后台服务器
U	公共数据电子标签
S	用户读写器
ID_U	公共数据电子标签的真实身份标志
$ID'_{U,old}$	公共数据电子标签的前一轮临时身份标志
$ID'_{U,new}$	公共数据电子标签的本轮临时身份标志
b_m	公共数据电子标签与用户读写器的同步化随机数
(PUF_m, PUF_{m+1})	PUF 函数的初始验证对
$Key_{j,new}$	公共数据电子标签与用户读写器的本轮共享密钥
$Key_{j,old}$	公共数据电子标签与用户读写器的前一轮共享密钥
$PUF(\cdot)$	随机置换函数
$\oplus$	按位异或运算
M_j	用户读写器生成的随机数
CRC	循环校验函数
$A_1 \sim A_5$	公共数据电子标签与用户读写器之间的交换信息

基于轻量级双向认证协议的公共数据安全防护结构如图 1 所示。

假设公共数据存储和传输过程涉及后台服务器 R 、用户读写器 S 及公共数据电子标签 U 三方,通过应用轻量级双向认证协议,实现用户读写器与公共数据电子标签的双向身份认证,优化公共数据存储和传输过程的安全防护效果。基于轻量级双向认证协议的公共数据安全优化算法整体流程如下所示。

(1) 在轻量级双向认证协议的初始化阶段,后台服务器 R 生成随机数 b_m 、密钥 Key_1 、密钥 Key_2 及 PUF 验证对 (PUF_m, PUF_{m+1}) ,并存储至用户读写器 S 中;公共数据电子标签 U 中存储其真实身份标志 ID_U 、临时身份标志 ID'_U 、随机数 b_m 、密钥 Key_1 及密钥 Key_2 。

(2) 用户读写器 S 将“Hello”消息发送至公共数据电子标签 U ,开始双向身份认证。

(3) U 接收 S 发送的消息后,向 S 传送其临时

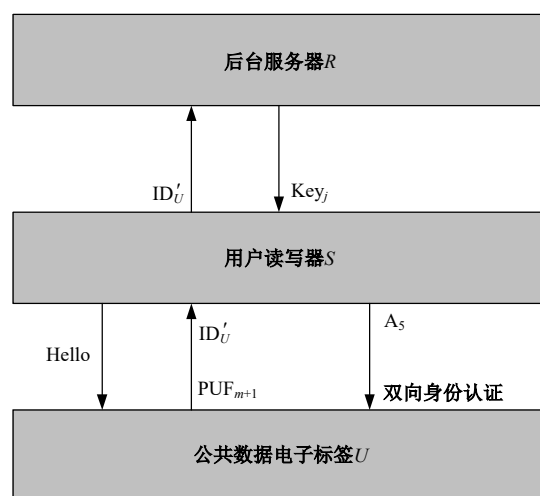


图 1 基于轻量级双向认证协议的公共数据安全防护结构图

Fig. 1 Structure diagram of public data security protection based on lightweight bidirectional authentication protocol

身份标志 ID'_U , S 将此临时身份标志传输至后台服务器 R 的数据库并实施搜寻。如果搜寻到与此临时身份标志相对应的标志,那么 R 会向 S 传送匹配该标志的密钥 Key_j ;反之,则判定身份认证失败,需返回重新实施身份认证。

(4) 在双向身份认证过程中^[12], S 生成随机数 M_1 和 M_2 ,对 S 与 U 之间的交换信息 A_1 和 A_2 进行运算后,将运算结果传送至 U ,请求 U 通过 PUF 运算实施验证。在此基础上, S 对其与 U 的同步化随机数 b_{m+1} 进行运算,有:

$$b_{m+1} = \text{CRC}(b_m \oplus M_1) \quad (1)$$

式中: $\text{CRC}(\cdot)$ 为循环冗余校验函数。

U 利用密钥 Key_1 、 Key_2 从交换信息 A_1 中提取 PUF_m ,用于后续 PUF 运算;同时通过这两个密钥和 PUF_m ,经运算得到交换信息 A_2 中的随机数 M_1 。

(5) U 依据 PUF_m 、 $PUF(\cdot)$ 函数及运算 $PUF(PUF_m)$ 所得的 PUF_{m+1} ,继续对 PUF_{m+2} 和 b_{m+1} 进行运算,其中 $PUF_{m+2} = PUF(PUF_{m+1})$;利用密钥 Key_1 、 Key_2 及 M_1 、 b_{m+1} 、 PUF_{m+1} 、 PUF_{m+2} ,运算 S 与 U 之间的交换信息 A_3 及二者的同步化随机数 B ,并将运算结果传递至 S 。 S 先从 B 中获取 U 传送的 PUF_{m+1} ,再与自身存储的 PUF_{m+1} 进行对比。若二者相同,则 S 对 U 的身份认证成功;反之,则身份认证失败。

(6) 身份认证成功后,继续利用密钥 Key_1 、 Key_2

及 M_1 、 b_{m+1} 、 PUF_{m+1} 对 A_3 中的 PUF_{m+2} 进行运算,并将 $(\text{PUF}_{m+1}, \text{PUF}_{m+2})$ 作为下一轮 S 身份认证和 U 的 PUF 验证对,随后更新 S 密钥。

(7) S 依据生成的随机数 M_2 对 S 与 U 之间的交换信息 A_4 、 A_5 进行运算,同时将运算结果传送至 U , U 从 A_4 中提取随机数 M_2 , 运算得出 $\dot{A}_5$, 并将其与 A_5 进行对比。若二者相同,则 S 获得 PUF_{m+2} , 且具备准确的同步化随机数 b_{m+1} , U 对 S 的身份认证成功,通过随机数 M_1 、 M_2 及 b_{m+1} 、 PUF_{m+1} 、 PUF_{m+2} 对用户读写器 S 密钥进行更新,完成协议认证;反之,则 U 对 S 的身份认证失败,不更新用户读写器 S 的密钥。

该优化算法中的认证协议通过同步化随机数实现用户读写器 S 与公共数据电子标签 U 的同步,可有效防御公共数据传输过程中的去同步化攻击。同时,该同步化随机数无需通过公共数据电子标签传送,可显著降低整体认证过程的通信量,有效适配复杂网络环境中海量多源数据的实时传输和存储需求,提升通信效率。另外,该协议通过引入 PUF 函数,显著提升了认证协议的整体安全性。即使攻击者获取某轮协议认证阶段的验证对 $(\text{PUF}_m, \text{PUF}_{m+1})$, 也不能以此为依据进行认证推理,使得公共数据电子标签认证较前期的循环校验函数(Cyclic redundancy check, CRC)更新所得密钥的安全性更高,实现了数据的安全防护。

1.2 基于可信网络连接的协议接入认证安全优化算法

本文算法是一种面向公共数据存储和传输场景,用于实现用户读写器与公共数据电子标签之间双向身份认证的解决方案^[13]。该算法在 1.1 节安全防护的基础上,于协议接入阶段引入可信网络连接,以认证用户读写器的可信度,同时完成用户读写器的加密注册,进一步预防攻击设备接入对公共数据安全造成的威胁^[14,15]。在此基础上,实施二者间的双向身份认证,提升公共数据传输过程的安全性,达到保护公共数据安全的目的。

基于可信网络连接的协议接入阶段用户读写器可信度认证过程如下所示。

(1) 用户读写器 S 向公共数据电子标签 U 发送接入请求,传送过程中, S 向 U 提供本轮请求申请方的随机数验证码 Code_s , 并携带其身份标志 ID_s , 便于 U 对其进行校对。为避免公共数据被窃听, ID_s 中需包含 U 校对后回复信息时使用的加密密钥 Key_s , 且 ID_s 中的全部信息均需通过 U

预先公布的公钥 pub_U 进行加密。该部分的方程式为:

$$S \rightarrow U: \{\text{Code}_s \| \text{ID}_s \| \text{Key}_s\}_{\text{pub}_U} \quad (2)$$

(2) U 接收注册消息并完成解密任务后,对消息的结构是否合法实施判别,若合法,则将此轮 S 接入请求过程中 U 的随机数验证码 Code_U 发送至 S 。期间,为提升安全性, U 向 S 发送的回复信息中需包含 S 请求时的验证码 Code_s 。此部分信息通过密钥 Key_s 实现加密,方程式为:

$$U \rightarrow S: \{\text{Code}_s \| \text{Code}_U\}_{\text{Key}_s} \quad (3)$$

(3) S 对 U 回复的随机数验证码与预先设定的随机数验证码进行一致性认证。若一致,则继续进入可信信息的传输和校验流程;若不一致,则结束用户读写器的接入。 S 将调用的可信度评估指标 CRE_s 打包后发送至 U ;在 U 向 S 传输公共数据的过程中,需包含 S 的状态信息 Status_s , 同时使用由 U 提出的验证码 Code_U 对传输过程中的连接状态进行校验。通过公钥 pub_U 加密此部分信息,加密方程式为:

$$S \rightarrow U: \{\text{Code}_U \| \text{Status}_s \| \text{CRE}_s\}_{\text{pub}_U} \quad (4)$$

(4) U 完成判别后,向 S 回复判别结果。期间, U 携带 S 的初始随机数验证码 Code_s 对本轮接入进行认证。通过密钥 Key_s 加密此部分信息,方程式为:

$$U \rightarrow S: = \{\text{Code}_s \| \text{Status}_s_End\}_{\text{Key}_s} \quad (5)$$

式中: End 表示认证结束。

2 实验结果分析

本文以某公共数据平台为例,选取 KDD-CUP99 数据集作为测试数据集,采用本文算法对该平台的公共数据进行安全防护优化,通过安全防护优化结果,检验本文算法的安全防护效果。实验环境如图 2 所示。

检验过程中,通过模拟中间人攻击、窃听攻击、去同步化攻击、数据篡改攻击、DDoS 攻击、克隆攻击、勒索软件攻击、追踪攻击、重放攻击及钓鱼攻击共 10 种攻击方式,对实验平台的公共数据存储和传输过程实施攻击。

2.1 不同方法的数据安全优化效果分析

为更好地检验本文算法的安全防护优化效果,选取差分隐私数据安全方法(文献[7]方法)、双账本数据安全方法(文献[8]方法)、区块链数据

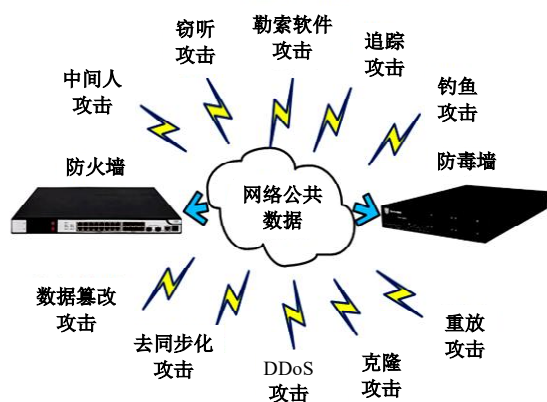


图 2 实验环境

Fig. 2 Experimental environment

安全方法(文献[9]方法)、区块联盟链数据安全方法(文献[10]方法)作为对比方法,分别对 10 种攻击方式下的实验公共数据进行安全防护优化,依据防护结果分析各方法的实际应用效果。各方法的安全防护优化结果如表 2 所示。

表 2 各方法的安全防护优化结果

Table 2 Safety protection optimization results of each method

攻击方式	本文算法	差分隐私方法	双账本方法	区块链方法	区块联盟链方法
中间人攻击	可抵抗	可抵抗	不可抵抗	可抵抗	可抵抗
窃听攻击	可抵抗	不可抵抗	可抵抗	可抵抗	可抵抗
去同步化攻击	可抵抗	可抵抗	可抵抗	不可抵抗	可抵抗
数据篡改攻击	可抵抗	可抵抗	不可抵抗	不可抵抗	可抵抗
DDoS 攻击	可抵抗	不可抵抗	可抵抗	可抵抗	可抵抗
克隆攻击	可抵抗	可抵抗	可抵抗	不可抵抗	可抵抗
勒索软件攻击	可抵抗	可抵抗	可抵抗	可抵抗	不可抵抗
追踪攻击	可抵抗	可抵抗	可抵抗	可抵抗	不可抵抗
重放攻击	可抵抗	可抵抗	不可抵抗	可抵抗	不可抵抗
钓鱼攻击	可抵抗	可抵抗	不可抵抗	可抵抗	可抵抗

分析表 2 可知,差分隐私方法无法抵抗公共数据存储和传输过程中的窃听攻击和 DDoS 攻击;双账本方法无法抵抗公共数据存储和传输过程中的中间人攻击、数据篡改攻击、重放攻击及钓鱼攻击;区块链方法无法抵抗公共数据存储和传输过程中的去同步化攻击、数据篡改攻击及克隆攻击;区块联盟链方法无法抵抗公共数据存储和传输过程中的勒索软件攻击、追踪攻击、重放攻击;而本文算法能够有效抵抗公共数据存储和传输过程中的 10 种攻击,对公共数据的安全防护效果更佳。

2.2 不同方法的数据安全优化时效性分析

公共数据的安全防护优化效果不仅需考虑对各种攻击的抵抗效果,还需考虑防护的时效性。为此,在上述实验的基础上,检验各方法在公共数据安全防护优化过程中的运算量、时延及通信量,以分析各方法的防护时效性。各方法在 10 种攻击方式下,对公共数据安全防护优化过程中 3 种检验指标的测试结果如图 3 所示。图 3 中,10 种攻击方式依次以编号 $a_1 \sim a_{10}$ 表示。

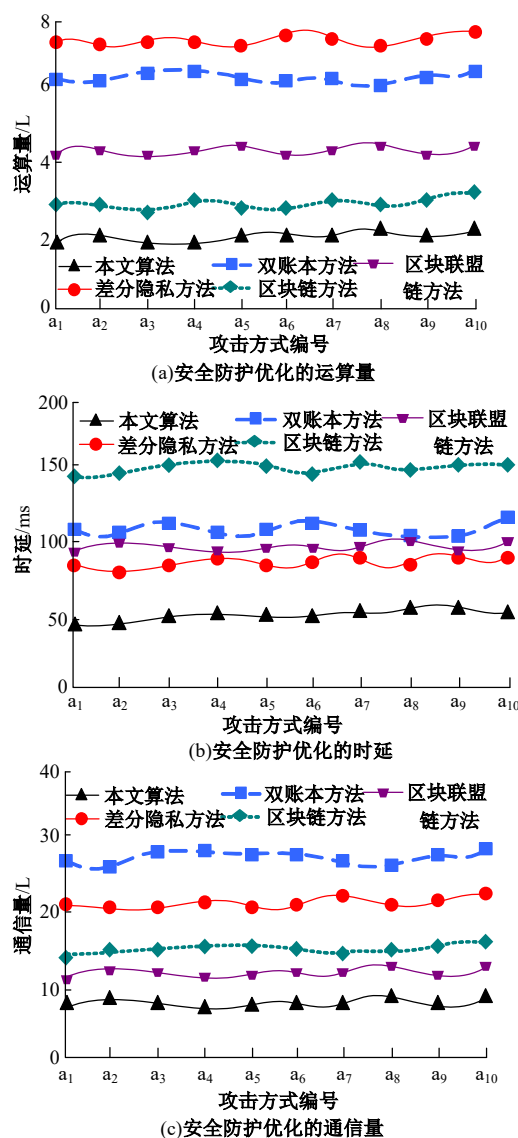


图 3 各方法安全防护优化中的检验指标值

Fig. 3 Test index values in security protection optimization of each method

由图 3 可知,在通信量方面,本文算法、区块链方法、区块联盟链方法较为接近,且明显低于另外两种方法;但区块联盟链方法的运算量过高,在该指标上表现不佳;而区块链方法的时延明显较

高,在该指标上表现不佳。综合分析,本文算法在10种攻击方式下对公共数据进行安全防护优化时,在通信量、运算量及时延方面均具有较好的表现,可满足公共数据安全防护的时效性需求,能及时应对各种攻击,保障公共数据的安全存储和传输。

3 结束语

公共数据具有多源性特点,其存储和传输过程的安全防护较为关键,为实现此目标,本文提出了一种应用轻量级双向认证协议的公共数据安全优化算法。该算法作为安全保护方案,采用轻量级双向认证协议,在公共数据存储和传输过程中实现高效的密钥管理和认证流程,不仅显著提高了公共数据的安全性,还降低了资源消耗,同时增强了隐私保护。实际应用结果表明,该算法可有效抵抗公共数据存储和传输过程中的各种攻击,且抵抗过程效率高、时延低,能够满足公共数据高效、精准的安全防护需求。

参考文献:

- [1] 刘海鸥,周颖玉,王海英. 基于区块链的突发公共卫生事件政府数据开放共享模型研究[J]. 现代情报, 2022, 42(10): 79-89.
Liu Hai-ou, Zhou Ying-yu, Wang Hai-ying. Research on open sharing model of government data of public health emergencies based on blockchain[J]. Modern Information, 2022, 42(10): 79-89.
- [2] 张利华,曹宇,张赣哲,等. 基于区块链的微电网数据安全存储与删除验证方案[J]. 计算机工程与设计, 2023, 44(4): 967-976.
Zhang Li-hua, Cao Yu, Zhang Gan-zhe, et al. Microgrid data security storage and deletion verification scheme based on blockchain[J]. Computer Engineering and Design, 2023, 44(4): 967-976.
- [3] 孔庆阳,何乐生,金浩男,等. 体测设备物联网数据安全传输机制的设计与实现[J]. 计算机应用, 2022, 42(增刊2): 180-185.
Kong Qing-yang, He Le-sheng, Jin Hao-nan, et al. Design and implementation of security transmission mechanism of Internet of Things data for physical measurement equipment[J]. Computer Application, 2022, 42(Sup. 2): 180-185.
- [4] 苏艳霞,王庆生,陈永乐. 基于数据分割的云存储中数据的安全共享[J]. 计算机工程与设计, 2021, 42(10): 2742-2747.
Su Yan-xia, Wang Qing-sheng, Chen Yong-le. Secure sharing of data in cloud storage based on data segmentation[J]. Computer Engineering and Design, 2021, 42(10): 2742-2747.
- [5] 程顺达. 基于安全性验证的云数据存储与访问算法[J]. 沈阳工业大学学报, 2023, 45(5): 565-570.
Cheng Shun-da. Cloud data storage and access algorithm based on security verification[J]. Journal of Shenyang University of Technology, 2023, 45(5): 565-570.
- [6] 康海燕,邓婕. 面向医疗数据安全存储的增强混合加密方法[J]. 北京理工大学学报, 2021, 41(10): 1058-1068.
Kang Hai-yan, Deng Jie. Enhanced hybrid encryption for secure storage of medical data[J]. Journal of Beijing Institute of Technology, 2021, 41(10): 1058-1068.
- [7] 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.
Wu Wan-qing, Zhao Yong-xin, Wang Qiao, et al. A method for safe storage and publication of trajectory data that satisfies differential privacy[J]. Computer Research and Development, 2021, 58(11): 2430-2443.
- [8] 赵骏,戴欢,唐毅,等. 基于双账本的物联网数据存储与共享方法[J]. 计算机工程与设计, 2023, 44(11): 3276-3282.
Zhao Jun, Dai Huan, Tang Yi, et al. Internet of things data storage and sharing method based on double ledger[J]. Computer Engineering and Design, 2023, 44(11): 3276-3282.
- [9] Li D, Han D Z, Crespi N, et al. A blockchain-based secure storage and access control scheme for supply chain finance[J]. Journal of Supercomputing, 2023, 79(1): 109-138.
- [10] 万征,丁超,余岚,等. 一种基于区块链的大健康数据存储和共享模型[J]. 小型微型计算机系统, 2023, 44(3): 636-645.
Wan Zheng, Ding Chao, Yu Lan, et al. A blockchain-based big health data storage and sharing model[J]. Small Microcomputer System, 2023, 44(3): 636-645.
- [11] 贺嘉琦,彭长根,付章杰,等. 面向RFID的轻量级双向认证协议[J]. 计算机工程与应用, 2023, 59(18):

- 268-277.
- He Jia-qi, Peng Chang-gen, Fu Zhang-jie, et al. Lightweight bidirectional authentication protocol for RFID[J]. Computer Engineering and Applications, 2023, 59(18): 268-277.
- [12] 陈飞鸿, 张锋, 陈军宁, 等. 基于RRAM PUF的轻量级RFID认证协议[J]. 计算机工程与应用, 2021, 57(1): 141-149.
- Chen Fei-hong, Zhang Feng, Chen Jun-ning, et al. Lightweight RFID authentication protocol based on RRAM PUF[J]. Computer Engineering and Applications, 2021, 57(1): 141-149.
- [13] 吴恺凡, 殷新春. 一种支持三方认证的轻量级RFID双向认证协议[J]. 小型微型计算机系统, 2022, 43(10): 2205-2213.
- Wu Kai-fan, Yin Xin-chun. A lightweight RFID bidirectional authentication protocol that supports three-party authentication[J]. Small Microcomputer System, 2022, 43(10): 2205-2213.
- [14] 郭奕旻, 张振峰, 熊平, 等. 基于PUF的轻量级雾辅助物联网认证协议[J]. 计算机学报, 2022, 45(7): 1412-1430.
- Guo Yi-min, Zhang Zhen-feng, Xiong Ping, et al. Lightweight fog assisted iot authentication protocol based on PUF[J]. Journal of Computer Science, 2022, 45(7): 1412-1430.
- [15] 吴斌, 严建峰. 基于区块链技术的分布式可信网络接入认证[J]. 计算机仿真, 2021, 38(1): 277-281.
- Wu Bin, Yan Jian-feng. Distributed trusted network access authentication based on blockchain technology[J]. Computer Simulation, 2021, 38(1): 277-281.