基于区块链的电子医疗数据安全共享方案

段嘉俊 柳 毅 陈家辉
(广东工业大学计算机学院 广东 广州 510006)

摘 要 随着医疗数据的急剧增长,如何实现电子医疗数据安全共享已成为电子医疗系统急需解决的问题。因此提出一种基于区块链的电子医疗数据安全共享方案,实现数据持有者和医疗研究机构的电子医疗数据安全共享,该方案采用零知识证明机制验证数据持有者的医疗数据是否符合医疗研究机构所需,采用同态加密技术保证医疗数据的安全性并实现密文的可操作性。理论分析表明使用该方案能满足保密性、可用性等安全保密要求,实验结果表明,采用该方案共享电子医疗数据所需计算花销更低。

关键词 区块链 安全共享 零知识证明 同态加密

中图分类号 TP309 **文献标志码** A DOI:10.3969/j.issn.1000-386x.2024.10.018

SECURE ELECTRONIC MEDICAL DATA SHARING SCHEME BASED ON BLOCKCHAIN

Duan Jiajun Liu Yi Chen Jiahui
(*School of Computers, Guangdong University of Technology, Guangzhou 510006, Guangdong, China*)

Abstract With the rapid growth of medical data, how to realize the secure sharing of electronic medical data has become an urgent problem for electronic medical system. Therefore, a secure sharing scheme of electronic medical data based on blockchain is proposed to realize the secure sharing of electronic medical data between data holders and medical research institutions. The scheme used zero knowledge proof mechanism to verify whether the medical data of data holders met the needs of medical research institutions, and used homomorphic encryption technology to ensure the security of medical data and realize the operability of ciphertext. Theoretical analysis shows that the scheme can meet the security requirements of confidentialityand availability. Experimental results show that using this scheme to share electronic medical data requires lower computational cost.

Keywords Blockchain Secure sharing Zero knowledge proof Homomorphic encryption

0 引 言

随着电子医疗系统的不断发展及可穿戴健康监控设备的不断进步,用户的体温、血压值、心率值、血氧饱和度等电子医疗数据呈几何式增长,对于医疗研究机构来说,这些健康指标数据是非常有助于研究社会总体健康状况的。通常情况下,数据持有者出于个人隐私的考虑,都希望对自己的医疗数据进行保密,即使数据持有者愿意向医疗研究机构披露部分医疗数据,在电子医疗数据的共享过程中,数据持有者仍然十分关注对医疗数据的隐私保护。因此,这是第一个需要解决的问题,即除了授权机构外,任何人无法访问数据持有者的医疗数据。

医疗研究机构若想通过健康指标数据得出社会总体健康状况的相关结论,需要提供所需医疗数据的关键信息,数据持有者得到关键信息后,可将自己的医疗数据生成可供医疗研究机构判定的凭证,随后医疗研究机构判断数据持有者共享的医疗数据是否符合分析所需,从而排除无关紧要的信息。因此第二个需要解决的问题是数据持有者如何在不泄露隐私信息的情况下向医疗研究机构证明他们的数据满足研究机构的要求。

此外,当医疗研究机构获取到数据持有者的电子医疗数据明文后,医疗研究机构可能会对电子医疗数据进行分析和挖掘,这会导致数据持有者的个人隐私

收稿日期:2021-04-06。**段嘉俊**,硕士,主研领域:区块链技术。**柳毅**,教授。**陈家辉**,讲师。

信息发生泄漏,如分析电子医疗数据中血糖值的波动情况可分析得到数据持有者的进餐时间等。因此如何防止医疗研究机构对医疗数据进行数据挖掘分析并保留电子医疗数据的可操作性是急需解决的第三个问题。

基于上述的挑战性问题,迫切需要一种解决方案来实现数据持有者和医疗研究机构之间的医疗数据安全共享,以保证数据持有者的隐私保护。因此本文提出一种基于区块链的安全共享方案,通过采用零知识证明机制验证数据持有者的医疗数据是否符合医疗研究机构所需数据的具体要求,同时采用同态加密技术对电子医疗数据进行加密处理,实现密文的可操作性。

1　国内外研究现状

由于医疗数据的爆炸式增长[1],传统的集中式医疗数据存储方案[2-4]已经无法满足数据可用性和可扩展性的要求,存在隐私泄露的风险。为了缓解数据存储压力,提高医疗服务质量,学者们[5-13]对区块链进行了大量的研究,以实现医疗数据的隐私保护分布式存储和安全共享。Vazirani 等[14]关注区块链的引入以及如何创建更高效的基础设施来管理电子病历,然而,他们没有提出一个具体的方案来实现在不损害患者的隐私安全的前提下改善医疗结果;Ivan 等[15]分析了利用区块链作为保护医疗数据隐私的存储方案的可行性,然而,他们在进行数据共享时忽略了身份管理和用户认证的问题;Bendia 等[16]提出了一种基于区块链的信任模型,该模型允许云服务提供商管理其信任关系,以便在不依赖可信第三方的情况下实现安全的数据共享;Li 等[17]提出了一种基于区块链的医疗数据保存方案,该方案在为数据所有者预先提供隐私服务的同时,确保电子医疗数据的原始性和可验证性,然而,医疗数据是由用户直接上传到系统中的,这对于大多数智能医疗场景是不适用的;为了保护患者的私人数据,Ibraimi 等[18]设计了一种细粒度 PHR 医疗服务公开方案,该方案是一种基于类型和身份的代理重加密方案,使委托人能够对其密文实施不同的访问控制策略;Fimiani 等[19]研究了通过使用改进的代理重加密方案实现医疗文档隐私保护共享的问题,其中密钥直接从用户的生物特征中提取;此外,在基于区块链的医疗平台中,交易的内容隐私性和共识效率也越来越受到关注。Li 等[20]采用环签名构建了基于椭圆曲线的隐私数据存储协议,保证了区块链应用中数据的安全性和用户身份的隐私性,然而,即使环签名解决了发送方和接收方的匿名性问题,也不能保护交易内容的隐私;Zheng 等[21]提出了一种结合区块链、云计算和机器学习的医疗数据共享方案,该方案可以方便地实现各医疗机构之间的医疗数据共享,然而,它无法验证云医疗数据的完整性,数据使用者也不确定是否收到了正确的医疗数据;Azaria 等[22]设计了一个基于以太坊的医疗信息共享平台,实现了医疗机构间医疗数据的分散安全集成,然而,方案中使用的一致性算法 PoW 需要非常高的计算负载才可维持区块链的一致性;Xue 等[23]提出了一种基于改进 DPoS 共识算法的医学区块链系统,可以降低节点的计算负载,提高数据共享的安全性和效率,但是,启动此模式至少需要 101 个医疗机构联邦成员服务器节点和 20 个审计联邦成员服务节点,而在共识的过程中,患者的隐私数据可能会被更多的节点获得;Huang 等[24]基于零知识证明和代理重加密对医疗研究机构能否获得满足需求的患者医疗数据,即对供需一致的数据可用性问题进行研究,但是医疗研究机构对密文解密后可获得患者的明文医疗数据,医疗研究机构可能会对患者的医疗数据进行数据分析从而获得患者隐私;Bai 等[25]提出了一种基于区块链的准同态对称加密方案来隐藏加密货币中的交易量。

通过对现有方案进行分析,可以发现区块链与医疗系统的结合有利于服务质量的提高,然而,不可忽视的是,数据持有者和医疗研究机构之间共享医疗数据的隐私保护仍然具有挑战性,特别是当实体之间共享数据涉及智能合约时,对隐私的综合考虑更是如此。而在数据持有者与医疗研究机构共享医疗数据后,医疗研究机构可以获得电子医疗数据明文,通过对医疗数据进行数据分析处理,可以获取到数据持有者的个人隐私。甚至,医疗研究机构可能会将医疗数据共享给未授权的机构导致泄漏数据持有者的电子医疗数据。

2　问题阐述

2.1　系统模型

系统模型:包括数据持有者、医疗研究机构、区块链、智能合约。

数据持有者:向医疗研究机构提供电子医疗数据的实体。

医疗研究机构:对医疗数据进行分析研究的实体。

区块链:记录数据持有者和医疗研究机构共享医疗数据过程的实体。

智能合约:自动执行零知识证明机制验证过程和同态加密运算过程的实体。

2.2 符号说明

本文所使用的符号说明如下:

EMD:电子医疗数据明文;SK_U:数据持有者私钥;PK_U:数据持有者公钥;SK_H:医疗研究机构的私钥;PK_H:医疗研究机构的公钥;$CEMD$:电子医疗数据密文。

3 预备知识

3.1 区块链技术

区块链技术是具有全网一致性共识、去中心化、可编程和安全防篡改等特点的分布式数据账本,区块链技术在 2008 年中本聪发表的《比特币:一种点对点的现金货币》中首次提出,是一种按照时间顺序存储的分布式共享数字账本。区块链利用加密块来验证和存储数据,利用 P2P 网络和共识机制来实现分布式系统的验证、通信和信任建立节点。区块链作为一种分布式账本,具有两个关键特性,即不变性和不可否认性。由于区块链具有的不变性和不可否认性,我们可以实现防止医疗数据的不可信或恶意修改,同时由于区块链具有可追溯性,因此可以对使用医疗电子数据的医疗数据机构进行记录和追溯。

智能合约可以在没有银行、法院或卫生部等外部实体监督的情况下提供自动化交易,从而促进安全可信的商业活动,实现复杂的区块链应用。

3.2 零知识证明机制

零知识证明是一个协议,证明人可以向验证人证明自己的价值知识,除了知道价值之外,不需要透露任何信息。零知识证明可分为交互证明和非交互证明。当应用到区块链中时,每个节点都必须检查交易的有效性,发送方与验证节点一起交换信息,因此区块链系统应该采用非交互证明。

zk-SNARK 满足必要的性质,包括完备性、稳健性和完全零知识,zk-SNARK 包含三个算法,分别为 ZKP-Keygen 算法、prove 算法和 Verify 算法。

3.3 Paillier 同态加密技术

Paillier 同态加密算法包含密钥生成算法 PKeygen、加密算法 PEncrypt、解密算法 PDecrypt。同时,Paillier 同态加密算法具有加法同态性,即存在:

$$x+y=D(E(x)\times E(y))$$

Paillier 同态加密算法的具体实现过程为:

1) PKeygen 算法:

(1) 随机选择两个大质数 p 和 q 使其满足:

$$gcd(pq,(p-1)(q-1))=1$$

(2) 计算 $n=pq$ 和 $\lambda=lam(p-1,q-1)$。

(3) 选择随机整数 $g(g\in Z_{n^2}^*)$,使得满足 n 整除 g 的阶。

(4) 公钥为(N,g)。

(5) 私钥为 λ。

2) PEncrypt 算法:

(1) 选择随机数 $r\in Z_n$。

(2) 计算密文,其中 m 为需要加密的信息:

$$c=\mathrm{PEncrypt}(m,r)=g^m r^n \bmod n^2, r\in Z_n$$

3) PDecrypt 算法:

$$m=\mathrm{PDecrypt}(c,\lambda)=(L(c^\lambda \bmod n^2)/L(g \bmod n^2))\bmod n$$

4 方案设计

4.1 基本思路

为了实现电子医疗数据的安全共享,本方案采用基于区块链对电子医疗数据进行共享,首先采用零知识证明机制对数据持有者的医疗数据进行验证,验证成功后使用同态加密技术对医疗数据进行加密运算操作,随后把输出结果加密传输给医疗研究机构。

4.2 方案流程

本方案的主要流程图如图 1 所示,具体步骤说明如下:

步骤 1 医疗研究机构根据满足其要求的医疗数据,通过 zk-SNARKs 算法生成一个零知识证明 π',然后将零知识证明 π'、相关计算结果 R'和散列值 h'记录到智能合约上,智能合约会把这些记录写入区块链中了,同时医疗研究机构会把需求中的一些关键词列举出来,如血压、心率、血氧饱和度等。

步骤 2 当数据持有者认为自己的电子医疗数据符合医疗研究机构在区块链网络中公开的关键词中的要求时,数据持有者可基于 EMD 生成可信的零知识证明 π,随后提交零知识证明给智能合约。

步骤 3 智能合约根据 Verify 算法分别对数据持有者和医疗研究机构上传的零知识证明、相关计算结果和哈希值进行比较。

步骤 4 若零知识证明验证成功,智能合约将提示数据持有者使用 PKeygen 算法生成公钥 PK_U 和私钥 SK_U,数据持有者需把生成的公钥及随机数上传到智能合约中,并生成电子医疗数据密文 CEMD,随后智能

合约将公钥及随机数上传到区块链进行共识认证;若验证不成功则取消此次数据共享。

步骤 5　智能合约通知医疗研究机构使用 PEncrypt 算法对所需医疗数据的合理范围值进行加密处理,同时上传密文到智能合约。

步骤 6　智能合约将医疗研究机构上传的范围值密文传送给数据持有者,随后数据持有者将收到的密文与电子医疗数据密文进行同态运算操作,并对运算结果集进行转换操作。

步骤 7　数据持有者将运算结果集上传到智能合约,随后智能合约使用医疗研究机构的公钥 PK_H 对数据比较结果进行加密并传输给医疗研究机构。

步骤 8　医疗研究机构接收到智能合约传输的密文后使用自己的私钥 SK_H 对密文进行解密。

步骤 9　最终,智能合约将此次交易提交到确认结点,此次电子医疗数据共享的记录将会写入区块链中。

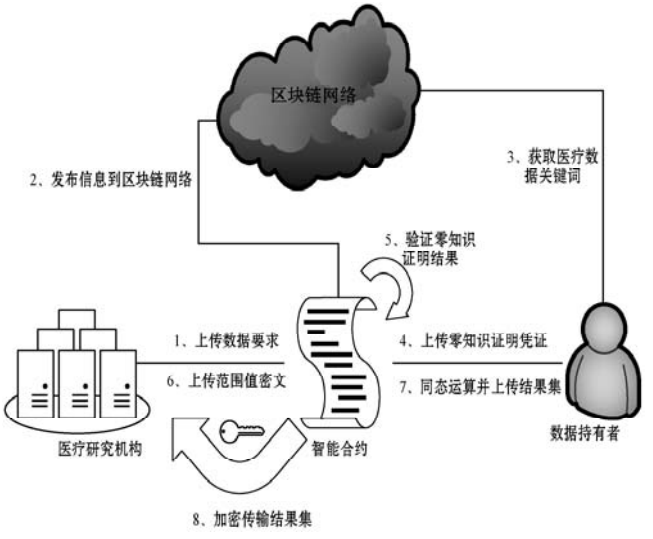

图 1　方案流程

4.3　零知识证明过程

数据持有者初步判断自己的医疗数据符合医疗研究机构的关键词后,数据持有者需要确认他的医疗数据是否确切符合医疗研究机构的条件,此时数据持有者需要生成零知识证明 π,随后智能合约需要对上传的证明凭证进行验证,详细步骤如下:

1)数据持有者创建运算模块:

$$C = \mathbb{F}^n \times \mathbb{F}^h \rightarrow \mathbb{F}^l$$

2)生成运算结果 R 和哈希值 h,向运算模块 C 中输入医疗数据集 $<m_1, m_2, \cdots, m_n, rd>$ 以及附加数据 $<ID, T>$,生成运算结果和哈希值,其中 ID、T、rd 分别为数据持有者的身份识别号、时间戳和随机数,运算结果和哈希值可用于验证数据的真实性和可用性,实现过程为:

$$C(<m_1, m_2, \cdots, m_n>) \rightarrow (R, h)$$

3)创建密钥对:输入安全参数 θ 和运算模块 C,输出用于生成零知识证明的密钥 GP_C 和验证零知识证明的密钥 VP_C:

$$\text{ZKPKeygen}(1^\theta, C) \rightarrow (GP_C, VP_C)$$

4)生成零知识证明凭证 π:

$$prove(GP_C, m, R, h) \rightarrow \pi$$

5)验证零知识证明:输入验证密钥、证明凭证、运算结果和哈希值进行验证操作,验证成功输出 True,否则输出 False:

$$Verify(VP_C, \pi, R, h) \rightarrow (True, False)$$

4.4　同态运算过程

对电子医疗数据进行同态运算,可以避免泄漏数据持有者的隐私信息,同时可以保证密文具有可操作性,同态加密运算的详细步骤如下:

1)医疗研究机构运行 PEncrypt 算法对健康指标合理范围值进行同态加密处理:

$$C_{\text{up}} = PEncrypt(range_{\text{up}})$$

$$C_{\text{down}} = PEncrypt(range_{\text{down}})$$

式中:$range_{\text{up}}$ 和 $range_{\text{down}}$ 分别为健康指标的合理范围的上限值和下限值。

2)数据持有者将范围值密文与电子医疗数据密文进行同态运算操作。

3)判断数据持有者提供的电子医疗数据健康指标值是否在医疗研究机构提供的合理范围值内,同时对输出结果集进行转换操作。转换规则为:若数据持有者的医疗数据值在指标的合理范围内则该项指标的数据置为 0;若医疗数据值高于合理范围则该项指标数据置为 1;若医疗数据值低于合理范围则该项指标数据置为 -1。

5　安全性分析

5.1　保密性

在本文的方案中,医疗研究机构上传到智能合约中的合理范围值以及数据持有者进行同态运算后得到的结果集都会通过安全加密算法进行加密,即使医疗研究机构上传的合理范围值产生泄漏,在没有获得解密密钥的情况下是没有办法对密文进行破解的。

5.2　隐私保护

在区块链网络注册时会对数据持有者和医疗研究机构进行严格检查,确保区块链的所有参与者都是合法的,随后可为每个参与者生成一个伪身份,因此,在

后续的共享过程中采用伪身份而不是真实身份,参与者的隐私将得到保护。而在数据共享过程中,任何参与智能合约交互的实体都不会泄露数据持有者的数据隐私,智能合约只能获得零知识证明 π 而不是原始的私有数据。此外,医疗研究机构只是发布一些关键词,而不是发布整个需求,这样可以实现部分隐私保护,也可以防止其他参与者根据医疗研究机构发布的需求伪造医疗数据。

5.3 可追溯性

当数据持有者和医疗研究机构达成共享电子医疗数据的共识后,此次共享电子医疗数据的行为将会记录到区块链中,如果任何一方有非法操作,例如,医疗研究数据将数据持有者共享的电子医疗数据结果集分享给未被授权的机构,将会被追究责任。

5.4 数据防分析

数据持有者对电子医疗数据密文以及健康指标范围值密文进行运算和比较后,会对输出结果集进行转换操作,最终输出的结果集会转换为 0、1、-1 的格式,因此医疗研究机构仅可得知数据持有者相关指标的大致情况,而无法得到具体数值以及波动情况,因此无法对结果集进行数据分析,从而保证了数据持有者的数据隐私安全。

5.5 可用性

只有获得授权的医疗研究机构才能使用他们的私钥来解密运算结果集。此外,数据持有者是基于自己的电子医疗数据生成完全可信的零知识证明 π,并提交给部署在区块链上的智能合约。基于零知识证明的特点,π 可以用来验证数据持有者的医疗数据是否符合医疗研究机构所需的医疗数据的要求,此功能通过供需的一致性匹配可以确保共享电子医疗数据的真实性和可用性。而医疗研究机构获取到输出结果集后,也可以通过结果集中相应指标上的 0、1、-1 值分析得到数据持有者此项指标的情况,从而可分析得到社会总体健康状况。

6 性能分析

实验环境:酷睿 i5-4200H,内存 12 GB,Windows 10 系统,编程语言为 Java,编程软件为 Eclipse Java。

本方案通过 Ganache 搭建以太坊私有链及创建账号,使用 MetaMask 钱包来对私有链进行测试,使用 Remix IDE 对智能合约进行开发、测试以及部署到私有链上,使用 web3.js 库提供的接口来调用智能合约、发起交易以及交易查看。

6.1 功能比较

通过和文献[22]、文献[23]以及、文献[24]等现有解决方案进行功能性的对比,可得知本方案可实现计算负载低、保护个人隐私、实现医疗技术数据共享的供需一致性以及防止数据分析等功能,对比详情如表 1 所示。

表 1 功能对比表

方案	低计算负载	隐私保护	数据供需一致性	防止数据分析
文献[22]	×	×	×	×
文献[23]	√	√	×	×
文献[24]	√	√	√	×
本文方案	√	√	√	√

文献[24]中采用了代理重加密技术对电子医疗数据进行加密处理,但是医疗研究机构对密文解密后可获得数据持有者的明文医疗数据,可能会对数据持有者的医疗数据进行数据分析或把医疗数据分享给未授权的医疗机构,这会导致数据持有者隐私的泄漏。

因此本文方案采用同态加密技术对电子医疗数据以及合理范围值进行加密,可以保证加密后的数据及范围值产生泄漏也无法被破解,同时可对密文进行同态运算。在同态运算后对输出结果集进行转换操作,可防止医疗研究机构对电子医疗数据进行数据分析获取到数据持有者的隐私信息,即使医疗研究机构将输出结果集分享给未授权的医疗机构,未授权的医疗机构也只能获取到经过转换操作的结果集,无法获取到数据持有者的隐私数据。

6.2 计算花销比较

文献[24]中使用了代理重加密方法实现数据持有者与医疗研究机构共享电子医疗数据,本文使用的同态加密技术实现数据持有者与医疗研究机构共享电子医疗数据,因此将对比数据持有者在文献[24]与本文中所需的计算花销。

在文献[24]中,数据持有者所需的计算花销为密钥初始化、数据加密、构造重加密密钥、密文重加密以及密文解密;而在本文中,数据持有者所需的计算花销主要为生成密钥、数据加密、密文运算、密文解密、输出结果集转换。

用于仿真实验的数据为日常监控的健康指标值,如体温、血压值、心率值、血氧饱和度等,健康指标数据以键值对的形式进行存储。在仿真实验中,文献[24]所用方案会读取所有健康指标项目及对应数值,随后对数据进行加密并输出密文。本文提出的方案会把每

一项健康指标值与合理范围值进行求和运算,判断该项健康指标值是否在合理范围内,随后会对判断结果集进行转换及加密。在仿真实验中,数据持有者与医疗研究机构共享的电子医疗数据所含的健康指标值的数量设定为 100、300、500 和 700 项,部分仿真数据如表 2 所示。

表 2　仿真数据

指标	体温/℃	血压值(收缩压)	血压值(舒张压)	血糖值
数值	36.9	110	70	5

日常需要的监控健康指标约有 200 项,从计算花销对比图中可以看出本文提出的电子医疗数据共享方案的计算花销低于文献[24],具体计算花销对比如图 2 所示。

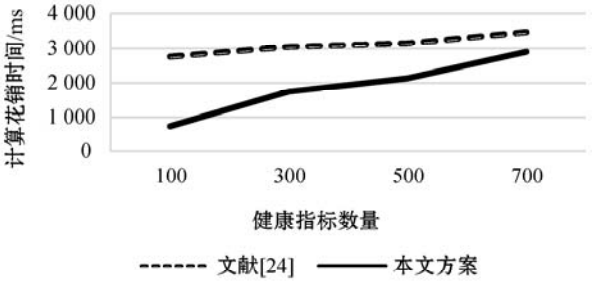

图 2　计算花销图

仿真实验的结果表明,采用本文方案在数据持有者与医疗研究机构共享日常健康指标等电子医疗数据所需的计算开销低于文献[24]中所使用的方案,而在本文方案中,对电子医疗数据采用同态加密算法进行加密操作以及对输出结果集进行了转换操作能更好地保护数据持有者的隐私信息,同时能更高效地实现数据持有者与医疗研究机构共享电子医疗数据。

7　结　语

根据对现有方案的分析,可以发现区块链与医疗系统的结合有利于服务质量的提高,不可忽视的是,数据持有者和医疗研究机构之间共享医疗数据的隐私保护仍然具有挑战性。基于这些挑战性问题,本文提出一种基于区块链的安全共享方案,通过采用零知识证明机制解决数据持有者和医疗研究机构对医疗数据的供需一致性问题,同时使用同态加密技术对医疗数据进行加密运算处理,达到避免医疗研究机构通过分析数据获得隐私的效果,理论分析可证明本文方案满足保密性、完整性、可用性等安全保密要求,实验结果表明本文方案的计算花销低于现有的解决方案,同时通过对输出结果集进行转换操作可避免医疗数据泄漏,可以实现在数据持有者与医疗研究机构之间安全高效地共享电子医疗数据。

参　考　文　献

[1] Liu L Y, Han M, Wang Y, et al. Understanding data breach: A visualization aspect[C]//13rd International Conference on Wireless Algorithms, Systems, and Applications, 2018.

[2] Zhang Y, Xu C X, Li H W, et al. HealthDep: An efficient and secure deduplication scheme for cloud-assisted eHealth systems[J]. IEEE Transactions on Industrial Informatics, 2018,14(9):4101 - 4112.

[3] Miao Y B, Tong Q Y, Choo K, et al. Secure online/offline data sharing framework for cloud-assisted industrial internet of things[J]. IEEE Internet of Things Journal,2019,6(5): 8681 - 8691.

[4] Liang J W, Qin Z, Xiao S, et al. Privacy-preserving range query over multi-source electronic health records in public clouds[J]. Journal of Parallel and Distributed Computing, 2020,135:127 - 139.

[5] 袁勇,王飞跃. 区块链技术发展现状与展望[J]. 自动化学报,2016,42(4):481 - 494.

[6] Mettler M. Blockchain technology in healthcare:The revolution starts here[C]//18th International Conference on e-Health Networking, Applications and Services,2016:1 - 3.

[7] Dorri A, Kanhere S, Jurdak R, et al. Blockchain for IoT security and privacy: The case study of a smart home[C]// IEEE International Conference on Pervasive Computing and Communications Workshops,2017:618 - 623.

[8] Zhang J, Xue N, Huang X. A secure system for pervasive social network-based healthcare[J]. IEEE Access,2016,4: 9239 - 9250.

[9] Zhu X Y, Badr Y. Identity management systems for the Internet of Things: A survey towards blockchain solutions[J]. Sensors,2018,18(12):4215.

[10] Yue X, Wang H J, Jin D W, et al. Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control[J]. Journal of Medical Systems,2016, 40(10):218.

[11] Panarello A, Tapas N, Merlino G, et al. Blockchain and IoT integration: A systematic survey[J]. Sensors,2018,18 (8):2575.

[12] Islam I, Munim KM, Oishwee SJ, et al. A critical review of concepts, benefits, and pitfalls of blockchain technology using concept map[J]. IEEE Access, 2020, 8: 68333 - 68341.

[13] Puthal D, Malik N, Mohanty SP, et al. The blockchain as a decentralized security framework[J]. IEEE Consumer Electronics Magazine,2018,7(2):18 - 21.

(下转第 226 页)

2010 IEEE International Symposium on Industrial Electronics,2010:2815 – 2820.
[2] Castro J, Delgado M, Medina J, et al. Intelligent surveillance system with integration of heterogeneous information for intrusion detection[J]. Expert Systems with Applications, 2011,38(9):11182 – 11192.
[3] Wang C, Zhang H, Yang L, et al. Deep people counting in extremely dense crowds[C]//23rd ACM International Conference on Multimedia,2015:1299 – 1302.
[4] Zhang Y, Zhou D, Chen S, et al. Single-image crowd counting via multi-column convolutional neural network[C]// 2016 IEEE Conference on Computer Vision and Pattern Recognition,2016:589 – 597.
[5] Li Y, Zhang X, Chen D. CSRNet: Dilated convolutional neural networks for understanding the highly congested scenes [C]//2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition,2018:1091 – 1100.
[6] Guo D, Li K, Zha Z, et al. DADNet: Dilated-attention-deformable convnet for crowd counting[C]//27th ACM International Conference on Multimedia,2019:1823 – 1832.
[7] Zhu F, Yan H, Chen X, et al. A multi-scale and multi-level feature aggregation network for crowd counting[J]. Neurocomputing,2021,423:46 – 56.
[8] Wang Z, Xiao Z, Xie K, et al. In defense of single-column networks for crowd counting[EB]. arXiv:1808.06133,2018.
[9] 杜培德,严华. 基于多尺度空间注意力特征融合的人群计数网络[J]. 计算机应用,2021,41(2):537 – 543.
[10] 王徐庆. 基于多尺度信息与注意力机制的人群密度估计算法研究[D]. 合肥:安徽大学,2020.
[11] 左健豪,姜文刚. 自适应融合特征的人群计数网络[J]. 计算机工程与应用,2021,57(21):203 – 208.
[12] Boominathan L, Kruthiventi S, Babu R. CrowdNet: A deep convolutional network for dense crowd counting[C]//24th ACM International Conference on Multimedia, 2016:640 – 644.
[13] Sam D, Surya S, Babu R. Switching convolutional neural network for crowd counting[C]//2017 IEEE Conference on Computer Vision and Pattern Recognition,2017:4031 – 4039.
[14] Dai F, Liu H, Ma Y, et al. Dense scale network for crowd counting[EB]. arXiv:1906.09707,2019.
[15] Huang G, Liu Z, Laurens V, et al. Densely connected convolutional networks[C]//2017 IEEE Conference on Computer Vision and Pattern Recognition,2017:2261 – 2269.
[16] Wang S, Lu Y, Zhou T, et al. SCLNet: Spatial context learning network for congested crowd counting[J]. Neurocomputing, 2020,404:227 – 239.
[17] Peng S, Wang L, Yin B, et al. Adaptive weighted crowd receptive field network for crowd counting[J]. Pattern Analysis and Applications,2020,24:805 – 817.
[18] Sindagi V, Patel V. Multi-level bottom-top and top-bottom feature fusion for crowd counting[C]//2019 IEEE/CVF International Conference on Computer Vision,2019:1002 – 1012.
[19] Idrees H, Saleemi I, Seibert C, et al. Multi-source multi-scale counting in extremely dense crowd images[C]//2013 IEEE Conference on Computer Vision and Pattern Recognition,2013:2547 – 2554.

(上接第 121 页)

[14] Vazirani A, Odonoghue O, Brindley D, et al. Blockchain vehicles for efficient medical record management[J]. NPJ Digital Medicine,2020,3(1):1 – 5.
[15] Ivan D. Moving toward a blockchain-based method for the secure storage of patient records[EB/OL]. [2021 – 03 – 21]. https://www. healthit. gov/sites/default/files/9-16-drew_ivan_20160804_blockchain_for_healthcare_final. pdf.
[16] Bendiab K,Kolokotronis N, Shiaeles S,et al. A novel blockchain-based trust model for cloud identity management [EB]. arXiv:1903.04767,2019.
[17] Li H Y, Zhu L H, Shen M, et al. Blockchain-based data preservation system for medical data[J]. Journal of Medical Systems,2018,42(8):1 – 13.
[18] Ibraimi L, Tang Q, Hartel P H, et al. A type-and-identity-based proxy re-encryption scheme and its application in healthcare[C]//5th VLDB Workshop on Secure Data Management,2008:185 – 198.
[19] Fimiani G. Supporting privacy in a cloud-based health information system by means of fuzzy conditional identity-based proxy re-encryption (FCI-PRE)[C]//2nd International Conference on Advanced Information Networking and Applications Workshops,2018:569 – 572.
[20] Li X F, Mei Y R, Gong J, et al. A blockchain privacy protection scheme based on ring signature[J]. IEEE Access, 2020,8:76765 – 76772.
[21] Zheng X C, Mukkamala R, Vatrapu R, et al. Blockchain-based personal health data sharing system using cloud storage [C]//20th International Conference on e-Health Networking, Applications and Services,2018:1 – 6.
[22] Azaria A, Ekblaw A, Vieira T, et al. MedRec: Using blockchain for medical data access and permission management[C]//International Conference on Open & Big Data, 2016:25 – 30.
[23] 薛腾飞,傅群超,王枞,等. 基于区块链的医疗数据共享模型研究[J]. 自动化学报,2017,43(9):1555 – 1562.
[24] Huang H P, Zhu P, Xiao F, et al. A blockchain-based scheme for privacy-preserving and secure sharing of medical data[J]. Computers & Security,2020,99:102010.
[25] Bai S J, Yang G, Rong C M, et al. QHSE: An efficient privacy-preserving scheme for blockchain-based transactions [J]. Future Generation Computer Systems,2020,112:930 – 944.