doi: 10.12068/j.issn.1005-3026.2020.03.007

基于区块链的无线体域网数据云存储完整性研究

高艳芳, 姚 兰, 马衍崧, 李凤云
(东北大学 计算机科学与工程学院, 辽宁 沈阳 110169)

摘 要: 针对无线体域网数据云存储的安全问题,设计了基于区块链的访问控制框架,框架通过区块链技术与数字签名相结合控制用户的访问请求;通过区块存储访问请求及其数字签名,利用改进的Raft算法保证节点间的区块链一致.其次,设计了有序数组和Merkle树相结合的方式存储数据,哈希表和Merkle树相结合的方式存储数据的访问请求;再次,提出针对无线体域网数据的完整性验证方案.最后,对区块链的一致性、数据完整性验证方案进行实验.结果表明,提出的框架能使各用户节点协同对访问请求进行控制,并且均能验证数据的完整性.

关 键 词: 区块链;无线体域网;完整性;Merkle树;数字签名
中图分类号: TP 309.2 **文献标志码**: A **文章编号**: 1005-3026(2020)03-0337-06

Research on Cloud Storage Integrity of Wireless Body Area Network Data Based on Blockchain Technology

GAO Yan-fang, YAO Lan, MA Yan-song, LI Feng-yun
(School of Computer Science & Engineering, Northeastern University, Shenyang 110169, China. Corresponding author: YAO Lan, E-mail: yaolan@mail.neu.edu.cn)

Abstract: Aiming at the security problems in cloud storage of the data in wireless body area network (WBAN for short), an access control framework based on blockchain was designed. The framework controlled user's access requests by combining blockchain technology with the digital signature. It used blocks to store access requests and digital signatures of the access requests, and utilized the improved Raft algorithm to ensure the consistency of each node's blockchain. Then, an ordered array combined with Merkle tree was designed to store WBAN data. A Hash table is combined with Merkle tree to store the access requests of the WBAN data. Thirdly, on the basis of access control framework, the storage mode of the WBAN data and the access requests of the WBAN data, and the integrity verification scheme for the WBAN data was proposed. Finally, experiments were carried out on the consistency of blockchain and the data integrity verification scheme. The experimental results showed that the proposed framework enables each user node to control the access request cooperatively, and the proposed scheme supports each user node to verify the integrity of data.

Key words: blockchain; wireless body area network (WBAN); integrity; Merkle tree; digital signature

无线体域网(wireless body area network, WBAN)是以人体为中心的小型网络[1].WBAN通过在人体的皮肤表面、衣物、人体周围嵌入的传感器节点收集人体生理信息.WBAN收集的人体血压、心电、体温、脑电波甚至血液参数等各种信息,被视为个人敏感数据[2],这些数据被医院、学校、政府部门、疾病研究机构等许多行业使用.随着WBAN的发展,WBAN产生了大量的数据,但WBAN节点的存储能力有限,将WBAN数据上传到云服务器存储可以解决WBAN不能存储大量数据的问题[3-4].

WBAN数据上传到云存储服务器时,数据被

收稿日期: 2019-03-05
基金项目: 国家自然科学基金资助项目(61602106); 中央高校基本科研业务费专项资金资助项目(N181604015).
作者简介: 高艳芳(1983-),女,辽宁营口人,东北大学博士研究生.

多用户共享,数据不再是本地存储和计算,完全受控于云服务器,使得存储在云服务器上的数据面临着以下严重的安全挑战.

1) 数据在上传到云服务器的过程中,可能受到恶意的拦截和篡改.

2) 人体参数的各项数据通常具有隐私性,数据存储在云上时,需要保证数据对云存储服务商的不可见,否则云存储服务商可能会对数据恶意传播,数据隐私性将遭到破坏.

3) 假设云存储服务商不可信,可能由于自身利益等原因,对云服务器上使用频率低的数据进行修改和删除,使数据的完整性遭到破坏.

4) 对于未授权的机构要避免其访问数据. 云存储数据由于多方共享,授权的不同机构对数据处理有着不同的要求,如何多方协调处理数据,避免单独机构在未经多方同意的情况下修改数据也是当前面临的重要问题之一.

区块链技术革命性地解决了“拜占庭将军问题”,具有不可更改、不可伪造、完全可追溯的安全特性,实现了一种无信任的共识网络系统[5-6]. 区块链系统一般由应用层、合约层、激励层、共识层、网络层、数据层等 5 个部分组成[7]. 区块链技术具有分布式存储和共识机制,对于解决访问控制和完整性验证两方面的安全问题都具有优势.

1 基于区块链技术的访问控制方法

针对数据的访问控制问题,基于区块链技术设计了如图 1 所示的访问控制框架. 框架中有数据上传者(DUP)、数据访问者(DAP)、数据操作授权中心(DAAC)、区块链网络(BCN)、云存储服务商(CSSP)等 5 种角色. BCN 逻辑上是由集合 $U=\{U_1,U_2,U_3,\cdots,U_n\}$ 构成的区块链网络;物理上,U_i 是已经被 DAAC 授予云存储服务的用户节点,U_i 使用区块链存储访问请求,U_i 具有 DUP 和 DAP 的双重身份,能够进行数据上传和访问,U_i 可提出访问请求、进行访问控制和验证 BCN 对访问请求的控制结果.

在本框架中,各节点密钥的生成及签名方式,采用无可信中心的数字签名方法[8]. 密钥生成首先需要进行数据初始化,H 为一个单向哈希函数,(P,P') 为两个安全的大素数,g 为 GF(P)阶,为 P'的生成元,$2^{511}<P<2^{512}$. Q 为 $P'-1$ 的素因子,α 为 GF(P')上的阶为 Q 的生成元,$2^{159}<Q<2^{160}$,BCN 用户节点集合 $U=\{U_1,U_2,U_3,\cdots,U_n\}$. 随后进行各节点密钥生成,对于用户节点 $U_i,i\in[1,n]$,Id_i 为 U_i 的唯一标识号,$\mathrm{Id}_i\in[1,Q-1]$,Id_i 对 BCN 的用户节点公开. 集合 U 中的每个用户节点构造 $f_i(x)=(a_0+a_1\times x+\cdots+a_{n/2+1}\times x^{n/2+1})\bmod Q$,$f_i(x)$ 为 $n/2+1$ 次多项式,其中$0<a_k<Q,k=0,1,2,n/2+1$,a_k 由 U_i 秘密保存,私钥 $\mathrm{SK}_i=\alpha^{f_i(0)}=a_0$,公钥 $\mathrm{PK}_i=g^{\alpha f_i(0)}\bmod P$,群公钥 $y=g^{\alpha f_1(0)\times\alpha f_2(0)\times\cdots\times\alpha f_n(0)}\bmod P$. U_i 为其他的用户成员 U_j 计算 $v_{ij}\,y_{ji}$,$v_{ij}\equiv\alpha^{f_i(\mathrm{Id}_j)}\bmod P'$,$y_{ji}\equiv g^{v_{ij}}\bmod P$,$U_i$ 将计算的 v_{ij} 和 y_{ji} 公开发送到 BCN 的其他用户节点.

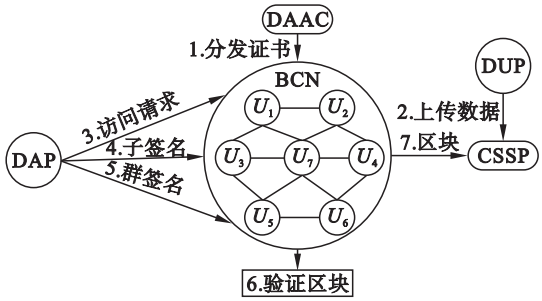

图 1 基于 BCN 的访问控制框架

Fig. 1 Access control framework based on BCN

各节点收到访问请求时,生成子签名,U_j 发送访问请求 O 到 BCN,BCN 的用户节点 U_i 查看访问请求 O,生成随机数 d_i,并计算 $r_i=\alpha^{d_i}$,发送 r_i 到 BCN,表示同意此访问请求. 同意访问请求 O 的用户节点构成集合 $U=\{U_1,U_2,U_3,\cdots,U_w\}$,如果 $w\geqslant n/2+1$ 表示 BCN 中超过 50% 的节点同意此访问请求. 同意访问请求 O 的节点 U_i 利用自己的密钥 SK_i 和各个节点收到的 $\alpha^{f_j(\mathrm{Id}_i)}$ 来生成子签名,子签名 s_i 如式(1)所示:

$$s_i=\left\{\left\{\alpha^{f_i(0)}\times\prod_{j\in U,j\notin B}\alpha^{f_j(\mathrm{Id}_i)\prod_{l\in B,l\neq i}\frac{-\mathrm{Id}_l}{\mathrm{Id}_i-\mathrm{Id}_l}}\right\}\times H(o)\times\alpha^{d_i}\right\}. \tag{1}$$

U_i 生成子签名后,选取随机数 k_i,满足 $\gcd(k_i,P')=1$,并计算 z_i,s_i',$z_i=g^{k_i}\bmod P$,$s_i'=k_i^{-1}(s_i-\alpha^{f_i(0)}\times z_i)\bmod P'$,此时 U_i 可将消息 $\{O,s_i,r_i,z_i,s_i'\}$ 发送给 U_j. U_j 收到各节点发来的子签名后,计算(R,S),式(2)计算 R,式(3)计算 S.

$$R\equiv\prod_{i=1,i\in B}^{n/2+1}r_i\bmod P', \tag{2}$$

$$S\equiv\prod_{i=1,i\in B}^{n/2+1}s_i\bmod P'. \tag{3}$$

此时 U_j 生成自己对访问请求 O 的数字签名,U_j 在区间$[1,P-1]$生成随机数 e_j,计算 $l_j,z_j,l_j=g^{e_j}\bmod P$,$z_j=(\alpha^{f_j(0)}\times O'-e_j\times l_j)\bmod(P-1)$,其中 $z_i\in[1,P-2]$,$O'=H(O)$. 随后 BCN 各节点可通过 $g^S\equiv y^{(O')^{n/2+1}\times R}\bmod P$ 验证群签名的真实

性,验证成功,则将访问请求存储到自己的区块中.

BCN 中的共识机制是通过改进 Raft 算法实现的. 首先通过心跳机制交互信息选取出记账人(Leader 节点),记账人随后通过区块链长度和区块链中最后一个区块的哈希值进行一致性判断,如果不相同,则进行区块补充,最终使得各节点区块链达到一致. Leader 节点使得 BCN 中各个节点的区块链达到一致后,当添加区块时,需要 BCN 各节点利用区块的哈希值对区块进行验证,如果 BCN 中大部分节点区块验证成功,则将区块记录. Leader 节点随后将区块发送至云存储服务器.

在本文设计的框架中,BCN 中各节点均可对请求进行投票,协同控制请求的有效性,并且通过区块记录请求. BCN 中通过改进的 Raft 算法,使得各节点的区块链一致,随后对区块的真实性进行验证,保证了上传到云存储服务中的区块是真实可信的.

2　基于区块链技术的完整性验证

2.1　区块的数据结构设计

WBAN 数据上传到 CSSP 进行存储,WBAN 感知数据的存储格式举例如表 1 所示. 体温、血氧、心率这些信息是 BCN 用户节点在某一时刻收集的,数据 D 表示为(数据号,用户号,体温,血氧,心率).

表 1　WBAN 感知数据格式

Table 1　The format of WBAN data

数据号	用户号	体温/℃	血氧/%	心率/(次·min^{-1})
160000	15110	37.5	95	65
160001	15012	36.0	92	80
160002	15057	36.5	90	70

CSSP 存储 WBAN 数据是通过数组节点之间数据号的间隔为 M 的有序数组和 Merkle 树相结合的方式. 有序数组每个位置对应 1 棵 Merkle 树,添加数据时只需修改数组节点对应的 Merkle 树即可;有序数组节点存储的是(数据号,Merkle 树根节点指针),M 表示 Merkle 树存储叶子节点数量的上限. Mekle 树节点分为内部节点和叶子节点,内部节点使用的哈希算法为 MD5,叶子节点使用的哈希算法为同态哈希算法. 内部节点包含的信息是(R,哈希值),叶子节点包含的信息是(R,哈希值,加密数据 D'),叶子节点的 R 为(D' 的数据号 - 对应有序数组节点数据号),内部节点的 R 为子节点中较大的 R. 叶子节点同态哈希值是使用文献[9]的同态哈希算法计算的.

数据 D(数据号,用户号,体温,血氧,心率)经过 SHK 加密后为数据 D'(数据号,用户号,SHK(体温),SHK(血氧),SHK(心率)),SHK 为 BCN 各节点使用的数据共享密钥用来加密数据,数据 D' 的数据部分 SHK(体温),SHK(血氧),SHK(心率),这三项数据可通过 $1 \times m$ 的矩阵 **FD** 表示,由于数据号、用户号作为主要唯一标识,不对其进行加密,所以初始化 $m = 3$,**FD** 表示如式(4)所示:

$$\mathbf{FD} = \begin{bmatrix} d_1 \\ d_2 \\ d_3 \end{bmatrix}. \tag{4}$$

其中,修改请求 X(数据号,SHK(血压),SHK(体温),SHK(心率))的数据部分可通过矩阵 **FX** 表示,如式(5)所示:

$$\mathbf{FX} = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}. \tag{5}$$

当 CSSP 处理修改请求 X 时,根据 X 中的数据号找到加密数据 D' 后,计算 $D' + X = D''$,数据部分相加如式(6)所示:

$$\mathbf{FD} + \mathbf{FX} = (d_1 + x_1, d_2 + x_2, d_3 + x_3). \tag{6}$$

可证明得到 $h_K(\mathbf{FD} + \mathbf{FX}) = h_K(\mathbf{FD}) \times h_K(\mathbf{FX})$,即算法满足乘法同态,其中 K 为同态哈希密钥. 当 CSSP 设置 M 为 4 时,存储结构如图 2 所示.

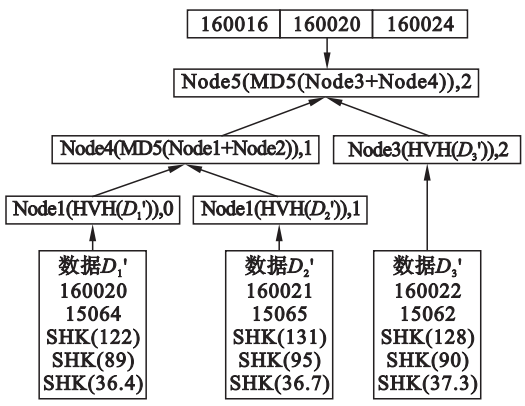

图 2　CSSP 存储结构图

Fig. 2　The diagram of CSSP storage structure

区块链由区块链式连接而成. 区块头部分包含父哈希——上一区块哈希值;时间戳——区块确实存在某一时刻;Merkle 树根节点哈希——区块中的 Merkle 树经过运算得到的根节点哈希值;当前区块哈希——MD5(父哈希 + 时间戳 +

Merkle 树根节点哈希). 每次区块生成时,首先将上一个区块的哈希作为父哈希,然后计算当前区块哈希,通过父哈希与上一个区块相连,形成链式结构.

区块体包含 Merkle 树——当要将区块加入到区块链中时,通过哈希表中存储的访问请求生成 Merkle 树;哈希表——访问请求经过 BCN 验证成功后将被放入到区块的哈希表;认证路径数组——Merkle 树叶子节点的认证路径的二维数组表示. Merkle 树的叶子节点存储访问请求. 初始区块被称为创世区块,即每个 BCN 用户节点区块链的第一个区块. 其中 Merkle 树为空,父哈希值为空,时间戳为 BCN 统一规定的时间,哈希值为 MD5 算法处理时间戳后得到的哈希值. 区块链结构如图 3 所示.

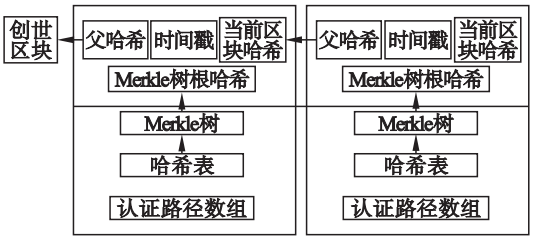

图 3 区块链结构

Fig. 3 The structure of blockchain

2.2 完整性验证

针对 BCN 的区块结构和 CSSP 存储 WBAN 数据的存储结构,利用同态哈希算法的同态特性对上传到 CSSP 的 WBAN 数据进行完整性验证. 本文中,由于 BCN 用户节点均存储访问请求,BCN 用户节点不需要委托可信第三方,即可对数据进行完整性验证,同时支持数据的动态操作.

1) 数据完整性验证模型. 数据完整性验证模型中的角色有上传节点 U_j 使用密钥 SHK 加密数据,使用同态哈希密钥 K 生成加密数据的哈希值,BCN 验证节点 U_i 随机选取数据号,进行数据验证,CSSP 存储加密数据,BCN 节点 U_k 返回认证路径,保证修改请求的可靠性. 数据验证模型如图 4 所示.

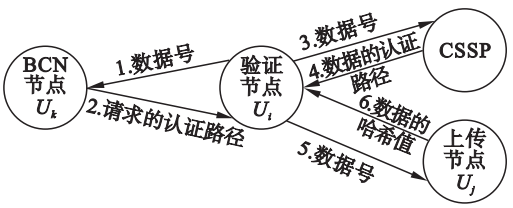

图 4 完整性验证模型

Fig. 4 The model of integrity verification

2) 数据完整性验证方案. 数据完整性验证方案由生成密钥(KeyGen),标签生成(TagBlock),挑战(Challenge),证据生成(ProofGen)和证据验证(Verify)5 部分组成,说明如下:

① 密钥生成阶段:密钥生成算法 DAAC 采用同态加密算法 Paillier 完成对密钥(PHK,SHK)的生成;

② 标签生成阶段:数据上传时,上传节点对加密后的数据 D' 进行同态哈希运算,生成标签 $h_K(D')$. 云存储服务器对数据进行存储,生成标签 $\mathbf{PD}(\mathrm{PD}_1,\mathrm{PD}_2,\mathrm{PD}_3,\cdots)$,$\mathbf{PD}$ 为在 CSSP 存储结构中数据 D' 的 Merkle 树的认证路径. BCN 用户节点 U_k 存储修改请求 X 时,生成标签 $h_K(X)$,$\mathbf{PX}(\mathrm{PX}_1,\mathrm{PX}_2,\mathrm{PX}_3,\cdots)$,$\mathbf{PX}$ 为修改请求 X 在区块结构的 Merkle 树中的认证路径;

③ 挑战阶段:验证节点 U_i 选取数据号 NM,并发送 NM 到数据上传节点 U_j,U_k,CSSP;

④ 证据生成阶段:CSSP 收到 NM 后,查找标签 $\mathbf{PD}(\mathrm{PD}_1,\mathrm{PD}_2,\mathrm{PD}_3,\cdots)$,将 $\mathbf{PD}$ 发回到 U_i,上传节点 U_j 收到 NM 后,查找标签 $h_K(D')$,将 $h_K(D')$ 发回给 U_i,BCN 用户节点 U_{ik} 收到 NM 时,查找修改请求数据号为 NM 认证路径 $\mathbf{PX}$,发送 $\mathbf{PX}$ 到 U_i;

⑤ 证据验证阶段:验证节点 U_i 收到 $\mathbf{PX}$ 后,U_k 可验证查找的标签 $h_K(X)$ 是否可靠. 假设 $\mathbf{PX}$ 是 3 维向量 $(\mathrm{PX}_1,\mathrm{PX}_2,\mathrm{PX}_3)$,$\mathrm{PX}_3$ 为区块中 Merkle 树根哈希,通过式(7)验证 $\mathbf{PX}$ 是否正确.

$$\mathrm{PX}_3=\mathrm{MD5}(\mathrm{MD5}(h_K(X)+\mathrm{PX}_1)+\mathrm{PX}_2). \tag{7}$$

如果式(7)成立,说明 U_i 查找的请求标签 $h_K(X)$ 正确,随后对数据完整性进行验证,假设 $\mathbf{PD}$ 是三维向量 $(\mathrm{PD}_1,\mathrm{PD}_2,\mathrm{PD}_3)$,$\mathrm{PD}_3$ 为 CSSP 存储结构中 Merkle 树根哈希,通过式(8)可对数据完整性进行验证.

$$\mathrm{PD}_3=\mathrm{MD5}(\mathrm{MD5}(h_K(X)\times h_K(D')+\mathrm{PD}_1)+\mathrm{PD}_2). \tag{8}$$

如果式(8)成立,说明 CSSP 存储的数据没有被恶意篡改,数据完整.

3 实验与结果分析

本文设计的框架主要是保证 BCN 用户节点能够协同控制对云存储数据的访问,保证云存储数据的安全. 下面针对框架的访问控制能力进行实验和安全分析,并对本文提出的数据完整性验证方案进行评估.

3.1　实验环境与实验数据

3.1.1　实验环境

本文的编程软件主要使用了 Pycharm，以 Linux 系统为平台，通过 Docker 容器模拟分布式环境的搭建，编程语言采用 Python，通过 Redis 数据库进行数据存储.

3.1.2　实验数据

本文的实验数据集使用的是已经脱敏的北京市某医院通过 WBAN 采集的病人生理信息数据，其数据构成如表 2 所示.

表 2　人体生理数据

Table 2　Human physiological data

病案号	体温/℃	血氧/%	心率/(次·min^{-1})	采集时间
126	37.5	90	65	2017－08－10 8:00
127	36.0	85	80	2017－08－10 8:10
126	37.5	91	73	2017－08－10 8:15
128	36.5	92	77	2017－08－10 8:15
129	35.5	96	74	2017－08－10 8:15
128	37.5	92	74	2017－08－10 8:20

表 2 所示的是部分病人的身体信息，由于这些数据只是单点采集，而本文讨论的是多个节点收集的 WBAN 感知数据的云存储，所以针对分布式的环境对数据格式进行了调整(格式见表 1)，其中用户号表示收集、使用数据节点节点号，数据号为数据在云存储中的唯一表示.

3.2　访问控制安全性分析及实验

数据隐私性：BCN 各节点将数据上传到 CSSP 时，利用共享密钥 SHK 对数据进行加密，保证数据对 CSSP 不可见.

抗单点安全：本文设计的框架保证了 BCN 用户节点提出的访问请求被多个 BCN 用户节点的协同控制，通过无可信中心的门限签名方法实现了控制权限的分配，访问请求只有通过 BCN 网络中大多数节点的同意才能被 CSSP 处理.

问责机制：BCN 用户节点提出访问请求时需要进行数字签名，访问请求经过多数 BCN 用户节点同意后，需要将访问请求和数字签名一起存储到区块中. 通过数字签名可以知道 BCN 网络中的哪个用户节点提出的访问请求.

区块验证：BCN 采用改进的 Raft 算法，Leader 节点维护 BCN 各用户节点区块链的一致，如果 Leader 节点伪造访问请求，则区块无法通过 BCN 其他用户节点的验证，验证失败，Leader 节点自动放弃记账权. 区块验证保证了 BCN 网络中 Leader 节点无法伪造访问请求，BCN 用户节点验证区块的基础是节点区块链长度保持一致，图 5 为 BCN 在选举出 Leader 节点后，BCN 各节点区块链长度随着时间的变化情况.

图 5 表明在 Leader 选举后的 100 ms 内，就能保证 BCN 各节点区块链的一致. BCN 节点区块链长度一致，说明各节点均参与了访问控制. 结果表明，设计的框架能够有效地保证数据的隐私性、访问请求的合理性，恶意的访问请求和未授权的访问请求均不能对云存储的数据加以访问，并且方便了追踪问责.

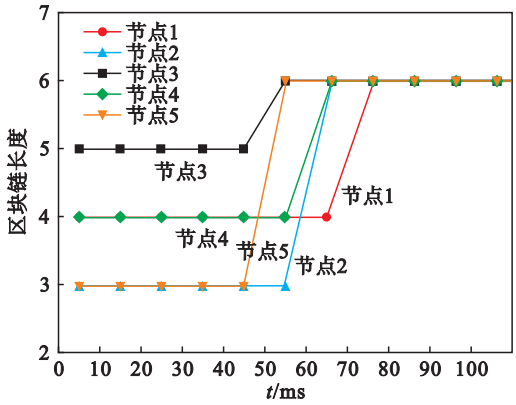

图 5　一致性维护

Fig. 5　Maintenance of consistency

3.3　数据完整性验证实验

在数据完整性验证的实验中，选取了多个节点对多条数据进行完整性验证，并对完整性验证结果进行统计. 图 6 是 BCN 用户节点对随机选取数据号进行完整性验证的结果，其中圆形节点表示验证成功，菱形节点表示验证失败. 实验结果表明，不同 BCN 用户节点对数据的完整性验证结果一致，表明完整性验证方案支持各用户均能进行完整性验证.

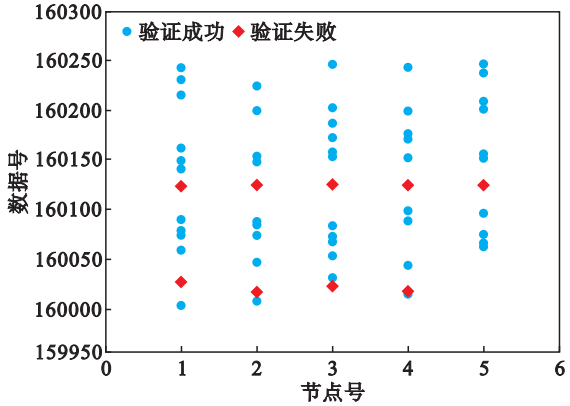

图 6　BCN 节点的数据完整性验证

Fig. 6　The data integrity verification of BCN nodes

4 结 语

针对 WBAN 数据存储在云服务器中存在的诸多安全问题,本文设计了基于区块链技术的访问控制框架,限制了多用户对云存储中 WBAN 感知数据的访问,之后在框架的基础上提出了数据完整性验证方案. 最后,对框架的安全性进行了实验和分析,并对所提出的数据完整性验证方案进行了实验评估,实验分析结果表明了方案的正确性、可行性,具有一定的理论和实用价值.

参考文献:

[1] Rahman A F A, Ahmad R, Ramli S N. Forensics readiness for wireless body area network (WBAN) system [C]// Proceedings of International Conference on Advanced Communication Technology. Piscataway: IEEE, 2014: 177 – 180.

[2] Kim Y, Lee S S, Lee S K. Coexistence of ZigBee-based WBAN and WiFi for health telemonitoring systems[J]. *IEEE Journal of Biomedical & Health Informatics*, 2015, 20(1): 222 – 230.

[3] He D, Zeadally S, Wu L. Certificateless public auditing scheme for cloud-assisted wireless body area networks[J]. *IEEE Systems Journal*, 2018, 12(1): 64 – 73.

[4] Li S, Hong Z, Jie C. Public auditing scheme for cloud-based wireless body area network[C]//Proceedings of IEEE/ACM International Conference on Utility & Cloud Computing. Piscataway: IEEE, 2017: 375 – 381.

[5] 谢辉,王健. 区块链技术及其应用研究[J]. 信息网络安全, 2016(9): 192 – 195.
(Xie Hui, Wang Jian. Study on block chain technology and its application[J]. *Network Security*, 2016(9): 192 – 195.)

[6] George P, Ilya S. Mechanising blockchain consensus[C]// Proceedings of 7th ACM SIGPLAN International Conference on Certified Programs and Proofs. New York: ACM, 2018: 78 – 90.

[7] 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.
(Yuan Yong, Wang Fei-yue. Blockchain: the state of the art and future trends[J]. *Acta Automatica Sinica*, 2016, 42(4): 481 – 494.)

[8] Krohn M N, Freedman M J, David M. On-the-fly verification of rateless erasure codes for efficient content distribution [C]//Proceedings of IEEE Symposium on Security & Privacy. Piscataway: IEEE, 2004: 226 – 240.

[9] Tsai T T, Tseng Y M, Hung Y H, et al. Cryptanalysis and improvement of a provable data possession scheme in public cloud storage [C]//Proceedings of Third International Conference on Computing Measurement Control & Sensor Network. Piscataway: IEEE, 2017: 56 – 59.

(上接第 310 页)

[9] Kwon S, Kim J. Real-time upper limb motion estimation from surface electromyography and joint angular velocities using an artificial neural network for human-machine cooperation [J]. *IEEE Transactions on Information Technology in Biomedicine*, 2011, 15(4): 522 – 530.

[10] Zhang F, Li P, Hou Z G, et al. sEMG-based continuous estimation of joint angles of human legs by using BP neural network[J]. *Neurocomputing*, 2012, 78(1): 139 – 148.

[11] 李小珉,尹明. 基于遗传算法的 BP 神经网络电子系统状态预测方法研究[J]. 电子测量技术, 2016, 39(9): 182 – 186.
(Li Xiao-min, Yin Ming. Research on the state prediction method of BP neural network electronic system based on genetic algorithm [J]. *Electronic Measurement Technology*, 2016, 39(9): 182 – 186.)

[12] 方晓柯,韩冰,朱雪枫,等. 基于速度场的上肢康复机器人的主动控制策略[J]. 东北大学学报(自然科学版), 2018, 39(2): 153 – 157, 171.
(Fang Xiao-ke, Han Bing, Zhu Xue-feng, et al. Active control strategy of upper limb rehabilitation robot based on velocity field [J]. *Journal of Northeastern University (Natural Science)*, 2018, 39(2): 153 – 157, 171.)

[13] Greff K, Srivastava R K, Koutnik J, et al. LSTM: a search space odyssey[J]. *IEEE Transactions on Neural Networks & Learning Systems*, 2015, 28(10): 2222 – 2232.

[14] Artemiadis P K, Kyriakopoulos K J. EMG-based control of a robot arm using low-dimensional embeddings [J]. *IEEE Transactions on Robotics*, 2010, 26(2): 393 – 398.