基金项目论文

基于区块链的社会网络用户属性差分隐私保护研究方案

汪林玉
（湖南科技职业学院，湖南长沙 410007）

摘　要：社会网络用户属性在互联网和大数据时代下，用户属性面临访问控制、隐私泄露、数据安全等问题，而传统的属性加密可以解决用户属性隐私保护过程中访问控制、信息获取问题，但仍存在访问数据安全、敏感信息泄露等挑战。基于以上问题，本文提出了社会网络用户属性隐私保护的方案，可以有效的防止社会网络用户访问控制时出现数据安全、隐私泄露问题。

关键词：区块链；差分隐私；隐私保护；用户属性
中图分类号：TP311.13　　**文献标识码：**A　　**DOI：**10.3969/j.issn.1003-6970.2022.04.017
本文著录格式：汪林玉.基于区块链的社会网络用户属性差分隐私保护研究方案[J].软件,2022,43(04):060-062

Research for the Blockchain-based Social Network with Differential Privacy Preserving of User Attribute

WANG Linyu
(Hunan Vocational College of Science and Technology, Changsha Hunan 410007)

【Abstract】: With the rapid development of Internet and big date, the social network user attribute has become more access captive, privacy disclosure and data insecure. Data privacy-preserving of access control and information acquisition can be solved by traditional encryption methods. However, there are still some challenges of data security access and sensitive information leakage. According to these problems and challenges, we proposed a blockchain technology to solve the social network with differential privacy-preserving of user attribute, which eliminates the data security and information leakage problems caused by social network user access control.

【Key words】: blockchain;differential privacy;privacy-preserving;user attribute

在大数据、互联网、信息共享的时代下，社会网络用户以其独特的身份占据了互联网用户一定的份额。社会网络用户数量多、信息丰富，那么隐私泄露的可能性就会越高。在这样的背景下，本文提出了基于区块链的社会网络用户属性差分隐私保护研究方案，将用户属性加密，数据资源加密上链，利用区块链进行交易保护，对交易用户的属性和数据资源进行保护，实现了用户隐私保护和数据安全保护。

属性加密可以保护用户的隐私信息，基于区块链结合属性加密，双重机制下保护用户隐私，进而实现隐私保护。如文献 [1] 提出基于节点分割的隐私属性匿名算法，通过分割节点的属性连接和社交连接，着重关注节点的匿名性。文献 [2] 提出一种基于属性加密的用户隐私保护云存储，对文件设置不同的访问权限，第三方使用 CP-ABE 方案将访问属性嵌入到密文中，当用户的属性满足密文的访问策略，可解密密文。文献 [3] 提出了基于区块链且支持验证的属性基搜索加密方案，通过对共享密钥采用密文策略属性加密机制，实现细粒度访问控制。文献 [4] 公开了一种保护隐私的基于 Merkletree 的区块链用户属性集核验方法，用户发布数据集合生成唯一标识，基于 Merkletree 确认用户数据合法签发，将节点数据的根哈希 Merklehash 和数据全局唯一标识绑定写入区块。

本文的主要贡献：

（1）将差分隐私结合用户属性加密，能够更有利的保护用户的隐私；

课题：2020 年湖南科技职业学院校级科研课题（KJ20221），课题名称：基于区块链的社会网络用户信息隐私保护研究
作者简介：汪林玉（1993—），女，湖南长沙人，硕士研究生，助教，研究方向：人工智能、社会网络和信息安全。

（2）利用区块链完成数据交易和监督过程，能够有效实现数据交易的安全性和透明性，区块链具有公开透明、不可篡改等特征；

（3）将用户属性加密和区块链进行组合的方案，能让用户的隐私保护和数据安全结合在一起，增加了用户和交易的双重安全性。

1 相关定义

1.1 差分隐私

数据集 x 是记录用户属性的集合，它来自于用户属性的全数据集 X($x \in X$)。将数据集 x 看成直方图向量，每个分量 x_i 代表数据集 x 中的一种记录出现的次数 $x \in N^{|X|}$，N 表示非负整数的集合。

定义 1 数据集之间的距离 数据集 x 的 l_i 范数表示为 $||x||_i$，表达式为：

$$||x||_i = \sum_{i=1}^{|X|} |x_i|$$

数据集 x 和 y 的 l_i 距离为 $||x-y||_i$。

定义 2 差分隐私 一个定义域 $N^{|X|}$ 的随机算法 M，如果对所有的 $H \subseteq Rang(M)$ 以及对所有满足 $||x-y||_i \leqslant 1$ 的数据集对 $x,y \in N^{|X|}$ 都满足：

$$Pr[M(x)] \in H \leqslant \exp(\varepsilon)Pr[M(y) \in H]+\delta$$

则 M 是满足 (ε,δ)- 差分隐私的。如果 δ=0，则 M 是 ε- 差分隐私。

定义 3 隐私损失

$$L_{M(x)||M(y)}^{(H)} = In\left(\frac{Pr(M(x) \in H)}{Pr(M(y) \in H)}\right)$$

当数据集 x 下事件的概率比在数据集 y 下的概率更大的情况下，隐私损失的值是正数值，反之，是负数值。

(ε,0)- 差分隐私保证了对所有相邻的数据集 x,y，隐私损失的绝对值小于等于 ε；

(ε,δ)- 差分隐私保证了对所有相邻的数据集 x,y，隐私损失的绝对值将以 1-δ 的概率小于等于 ε (δ 是失败概率)。

1.2 用户属性加密方案

用户属性加密是将标识用户身份的信息进行处理，根据属性访问的方式，制定与属性集相匹配的访问策略，访问用户只有满足访问策略才能解密密文得到明文。用户属性加密包括三个数据交易实体对象可信授权中心、数据请求者、数据拥有者，加密过程 [5] 如表 1 所示。

2 方案设计

2.1 方案模型

本方案实施过程中拥有一下实体：数据请求者、数据拥有者、社会网络、区块链。如图 1 所示。

（1）数据请求者：数据的消费者。数据请求者通过区块链提出数据交易请求，满足访问策略 [6] 或经过数据拥有者同意，可对区块链返回的密文进行解密操作。

（2）数据拥有者：数据的实际拥有者。制定访问控制策略的权限，决定可交易数据的资源；加密原始文件上传等。

（3）社会网络：互联网云端。支持社会网络成员上传加密的数据资源，成员间提供信息交流和一些列交互操作。

（4）区块链。交易链：接收属性加密的关键密文，利用差分隐私进行属性加密，支持数据交易过程，在交易过程中保护用户的隐私。

监督链：存储数据交易结果，支持查询和监督。

表 1 用户属性加密

Tab.1 User attribute encryption

属性加密过程（Attribute Encryption Process）
输入：隐私参数 ε、δ 失败概率
加密过程：
1. 区块链交易初始化算法 Init(ε,δ) → (PK,MK)：以隐私参数 ε 为输入，输出得到公钥 PK 和主密钥 MK。
2. 加密算法 Encrypt(PK,MK,A) → DK：以公钥 PK、主密钥 MK 和访问策略 A 为输入，输出加密密文 CT。
3. 属性加密密钥生成算法 Generate(PK,MK,X) → DK：以公钥 PK、主密钥 MK 和属性集合 X 为输入，输出解密密钥（私钥）DK。
4. 解密算法 Decrypt(PK,DK,CT) → DK：以公钥 PK、解密密钥 DK 和密文 CT 为输入，用户属性满足访问策略 A，输出对应属性集的明文 PT。

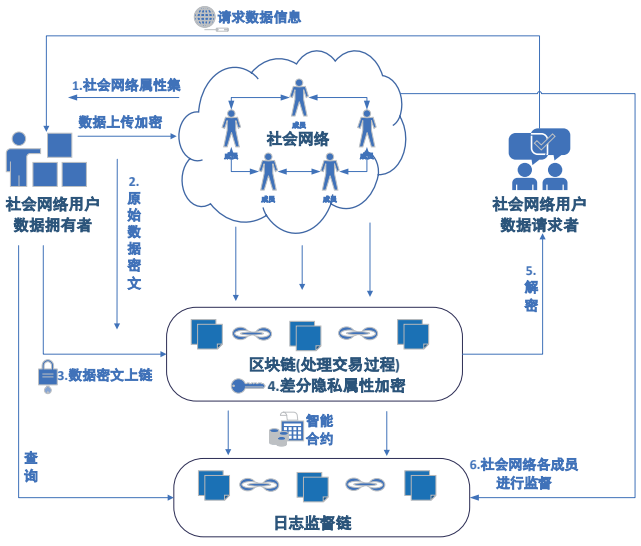

图 1 方案框架图

Fig.1 Scheme Framework

2.2 方案设计过程

根据方案的实现过程，可以将该方案分为三个阶段，如下：

（1）阶段 1：初始化。

初始化阶段分为隐私参数 ε 生成和密钥生成两个部分，具体过程如下页表 2 所示。

表 2 初始化过程

Tab.2 Initialization process

隐私参数 ε 生成（Privacy Parameter ε Generation）
输入：社会网络属性集 x，随机算法 M，
根据差分隐私计算得到 M 是 ε- 差分隐私
输出：差分隐私参数 ε、δ 失败概率
密钥生成（Key Generation）
输入：隐私参数 ε，δ 失败概率，初始化算法 Init。
用户属性加密方案，通过 1.2 该属性加密过程，进行秘钥生成
输出：加密密文 CT、解密密钥（私钥）DK、对应属性集的明文 PT

（2）阶段 2：数据交易。

数据交易阶段分为社会网络成员通过区块链进行数据交易和数据请求者解密数据的过程，具体过程如表 3 所示。

表 3 数据交易和解密过程

Tab.3 Data transaction and decryption process

数据交易（Data Transaction）
输入：原始数据加密密文 CT
关键密文上链，数据密文 CT、加密数据上传区块链
区块链处理交易过程：
1. 数据拥有者发出交易请求
2. 交易事务 TRADES
（1）数据拥有者定义一个资源请求访问控制策略 B
（2）区块链对数据拥有者数据交易生成 (公钥 GK、私钥 SK) 对、定义一个令牌 T
（3）区块链钱包处理：
1）访问控制策略 B 转换成脚本 S：B → S
2）数据请求者的公钥 GK 进行令牌加密，得到加密后的令牌 T'：T'=E(PK,T)
3）利用数据拥有者的私钥 SK 签署数字签名 SIGN
（4）广播交易请求到社会网络，通过社会网络传播
（5）数据拥有者的钱包对交易进行脚本锁定 L(S)，与区块链上的成员进行商量，允许交易后解锁脚本 U(S)
（6）资源请求者与社团其他成员进行协商，允许交易后，生成交易事务 TRADES(SIGN,T')
3. 区块链执行交易验证过程
输出：数据拥有者具备属性加密后的数据 Data
数据请求者解密数据（Data Requester Decryption）
输入:数据拥有者具备属性加密后的数据 Data、解密密钥（私钥）DK、访问策略 A
用户属性解密方案，通过 1.2 该属性解密过程，通过解密秘钥 DK、访问策略 A、解密出明文 PT
输出：明文 PT（解密属性后的数据）

表 4 数据监督过程

Tab.4 Data monitoring process

数据监督（Data Supervision）
交易会记录到区块链上的账本中，当交易过程出现问题时，可以进行复核然后进行复核，将处理结果签名后通过监督日志放到监督链上记录，以供区块链成员进行查看，实现分布式监管。

（3）阶段 3：数据监督

数据监督过程为社会网络成员通过区块链进行数据监督，具体过程如表 4 所示。

3 安全分析

3.1 安全性证明

定义：数据交易事务中的令牌加密、脚本锁定和数字签名可以防止恶意篡改数据。

证明：攻击点：（1）偷下载所需要的令牌；（2）恶意篡改。

保护点：（1）属性加密过程中会对数据属性进行加密，这是第一次加密。数据交易过程中数据请求者的公钥 GK 进行令牌加密，这是第二次加密。（2）数据拥有者的钱包对交易进行脚本锁定，与区块链上的成员进行商量，允许交易后解锁脚本。（3）利用数据拥有者的私钥 SK 签署数字签名 SIGN，所有的交易在区块链上都必须签署防止恶意篡改的外部用户合约 (智能合约)。

3.2 隐私保护

数据层面：对数据资源加密，然后上传到区块链，利用访问控制策略，符合访问控制策略才可得到解密秘钥，进行解密。

属性层面：利用差分隐私结合属性加密机制，对用户的属性进行处理和加密，从而隐藏真实的属性，保护用户的隐私。

区块链层面：该方案借助于区块链，区块链的成员都有唯一的公私钥对，进行数字签名，从而降低了区块链成员身份泄露和数据泄露，保护用户的安全。

4 结语

利用区块链，将数据信息加密上链，保证利用访问控制策略和属性 (数据) 加密实现了保护敏感隐私的交易过程，本文提出基于区块链的社会网络用户属性差分隐私保护研究方案，利用差分隐私，该方案能够实现保护用户隐私和数据交易的过程。

参考文献

[1] 付艳艳,张敏,冯登国,等.基于节点分割的社交网络属性隐私保护[J].软件学报,2014,25(4):768-780.

[2] 曹来成,刘宇飞,董晓晔,等.基于属性加密的用户隐私保护云存储方案[J].清华大学学报(自然科学版),2018,58(2):150-156.

[3] 闫玺玺,原笑含,汤永利,等.基于区块链且支持验证的属性基搜索加密方案[J].通信学报,2020,41(2):187-198.

[4] 陈宇翔,郝尧,董贵山,等.一种保护隐私的基于Merkletree的区块链用户属性集核验方法:中国:CN202010243336.6[P].2020-07-28.

[5] 李雪莲,张夏川,高军涛,等.支持属性和代理重加密的区块链数据共享方案[J/OL].西安电子科技大学学报:1-16[2022-04-18] .

[6] 王海斌,陈少真.隐藏访问结构的基于属性加密方案[J].电子与信息学报,2012,34(2):457-461.