Computer Science and Application 计算机科学与应用, 2022, 12(8), 1913-1921
Published Online August 2022 in Hans. http://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2022.128192

Hans汉斯

基于区块链的物联网数据访问控制方案

朱帅禎，曹　丽

临沂大学信息科学与工程学院，山东 临沂

收稿日期：2022年7月10日；录用日期：2022年8月10日；发布日期：2022年8月16日

摘　要

在万物互联的时代背景下，物联网飞速发展，无论从局部设备数量还是整体规模都呈现高速增长的趋势，随之而来的数据安全问题也日益凸显。属性基加密(ABE)是保护数据安全的核心技术之一。但是，将属性基加密方案应用到物联网环境中仍然面临着许多挑战。属性基加密基于双线性配对实现，这种基于线性配对实现的加密是是开销很高的操作，不适合资源受限的物联网设备。为了解决这个问题，本文提出了一种基于区块链的物联网数据访问控制方案，该方案借助智能合约技术，将属性基加密中开销高的双线性配对操作外包至区块链中执行，进行预解密，然后在本地验证区块链预解密的正确性，从而减轻了用户端的计算压力，解决了属性基加密应用于物联网环境开销高的问题，实现了轻量级的访问控制。安全分析结果表明，该方案在数据机密性、防篡改攻击和抵抗合谋攻击方面是可靠的。

关键词

属性基加密，访问控制，物联网，外包预解密，区块链

Blockchain-Based IoT Data Access Control Scheme

Shuaizhen Zhu, Li Cao

School of Information Science and Engineering, Linyi University, Linyi Shandong

Received: Jul. 10th, 2022; accepted: Aug. 10th, 2022; published: Aug. 16th, 2022

Abstract

In the era of the Internet of Everything, the IoT has developed rapidly, showing a rapid growth trend in both the number of local devices and the overall scale, and the accompanying data security issues have become increasingly prominent. Attribute-based encryption (ABE) is one of the core technologies to protect data security. However, applying attribute-based encryption schemes

文章引用: 朱帅禎, 曹丽. 基于区块链的物联网数据访问控制方案[J]. 计算机科学与应用, 2022, 12(8): 1913-1921.
DOI: 10.12677/csa.2022.128192

to the Internet of Things environment still faces many challenges. Attribute-based encryption is implemented based on bilinear pairing, which is considered to be an expensive operation and is not suitable for resource-constrained IoT devices. In order to solve this problem, this paper proposes a blockchain-based IoT data access control scheme. Through smart contract technology, the bilinear pairing operation with high cost in attribute-based encryption is outsourced to the blockchain for execution, and pre-decryption is performed and then locally verifies the correctness of blockchain pre-decryption, thereby reducing the computational pressure on the user side, solving the problem of high cost of attribute-based encryption applied to the IoT environment, and realizing light-level access control. The security analysis results show that the scheme is reliable in terms of data confidentiality, anti-tampering attacks and resistance to collusion attacks.

Keywords

Attribute-Based Encryption (ABE), Access Control, IoT, Outsourced Pre-Decryption, Blockchain

1. 引言

伴随物联网飞速发展而来的数据安全问题越来越凸显。物联网设备数量众多、规模庞大，产生的数据包含大量个人隐私，例如：智能摄像头捕获的音视频、可穿戴设备收集的个人信息等。如果数据严格管控，不与外界分享，则物联网强大的潜力不能发挥；而与外界分享数据时，所传输的数据会通过不受信任的网络路由或存储在不受信任的云服务器中。此外，传统互联网中，管理者可以在数据生成时为其提供完整性证明与身份验证，但是机密性通常由非对称加密来实现。与传统互联网不同的地方在于，物联网设备进行通讯时，数据管理者所传输的数据可能只希望某些选定方可以访问。物联网的数据分享通常需要一方加密多方解密，因此传统的访问控制方案很难适用于物联网环境。

区块链(Blockchain)技术[1]是由中本聪(Satoshi Nakamoto)在 2008 年首次提出来的。作为一种分布式点对点交易平台，由于其自身所具有的安全、可审计、可追溯、不可篡改等特性，区块链已经被认为是满足物联网安全需求最有前途的技术之一[2] [3]。虽然区块链是一项新兴技术，但已经有很多研究提出将区块链技术(如 Fabric [4] [5]、Bitcoin [1])应用到现有的访问控制方案中。一般来说，访问控制方案中区块链的使用可以分为两类，一是基于分布式账本实现去中心化存储，二是基于智能合约支持分布式服务。一方面，Zyskind [6]等提出将权限授予与检查作为区块链的底层交易协议，使得数据所有者可以更有效率地管理用户对其数据的访问；Hossein Shafagh [7]等使用区块链交易来存储访问权限信息，确保访问授权不会被篡改；Ouaddah [8]等提出的基于区块链的访问控制参考模型，扩展了 Fabric 底层交易结构，将数字货币用授权令牌替代，数字货币交易改为令牌的交易。因此，该模型可以通过令牌交易实现访问权限的授予、获取。另一方面，Zhang [9]等通过不同的以太坊智能合约管理每个主体(资源请求者)和客体(资源拥有者)之间的访问策略；Liu [10]等人将区块链与基于属性的访问控制(ABAC)相结合，以 Fabric 平台为基础，设计了三种智能合约来实现物联网访问控制；丁晟[11]等人提出了一种新的基于属性的物联网系统访问控制方案，使用区块链技术来记录属性的分布，以避免单点故障和数据篡改，大大简化了访问管理，并且对访问控制流程也进行了优化。

Sahai 和 Waters 提出的属性基加密(ABE)技术[12]同时实现了数据加密与访问控制，由于其细粒度、

一对多、用户控制等特点而被广泛应用于加密访问控制。与传统的密码算法相比，属性基加密提供了一种更高效的访问控制方案：在 Bethcourt 等人提出的密文策略属性基加密(CP-ABE) [13]中，数据请求者的私钥与其拥有的属性相关联，数据管理者将数据与访问结构封装形成密文，当且仅当私钥关联的属性满足密文的访问结构时，才能成功解密。在该方案中，数据请求者的身份由其所拥有的属性来描述，数据管理者只需要加密一次，满足访问结构的所有数据请求者就可以多次解密。然而，尽管属性基加密拥有显著的优点，但其计算开销对于物联网中资源受限型设备是一个巨大的挑战。定义访问结构所使用的属性的数量会显著影响属性基加密在实际应用中的性能：CP-ABE 中，生成访问结构需要为每条属性进行幂运算；解密与双线性配对操作有关。这两种操作在基于配对的密码学中开销很高，很难适用于资源受限性设备大规模存在的物联网环境。

基于以上问题，本文提出了一种基于区块链的物联网数据访问控制方案，该方案借助智能合约技术，将属性基加密中开销高的双线性配对操作外包至区块链中执行，进行预解密，然后在本地验证区块链预解密的正确性，从而减轻了用户端的计算压力，解决了传统访问控制方案中数据请求端开销高的问题，实现了轻量级的访问控制。

2. 预备知识

2.1. 双线性映射

设 G 与 G_S 是两个阶为素数 p 的乘法循环群，g 与 g_S 分别为两个循环群的随机生成元。定义运算 $e:G\times G_S\to G_T$ 为双线性映射，具有以下性质：

1) 双线性：$\forall a\in G,\forall b\in G_S,x,y\in Z_p,e\left(a^x,b^y\right)=e\left(a,b\right)^{xy}$。

2) 非退化性：$\forall a\in G,\forall b\in G_S,e\left(a,b\right)\neq 1$，1 为 G_T 单位元。

3) 可计算性：$\forall a\in G,\forall b\in G_S$，存在有效的多项式算法计算 $e\left(a,b\right)$。

若 $G=G_S$，则该映射对称，否则为非对称映射。

2.2. 访问结构

设 $\left\{p_1,p_2,\cdots,p_n\right\}$ 为参与方集合，集合 $\Upsilon\subseteq 2^{\left\{p_1,p_2,\cdots,p_n\right\}}$。对于 $\forall B,C$，若 $B\in\Upsilon$ 且 $B\subseteq C$，则 $C\in\Upsilon$，则 Υ 是单调的。若 $\Upsilon\subseteq 2^{\left\{p_1,p_2,\cdots,p_n\right\}}/\left\{\varnothing\right\}$，且单调，则 Υ 是一个访问结构(单调访问结构)。若集合 $D\in\Upsilon$，则称 D 为授权集，否则为非授权集。

本文采用单调访问结构，参与方集合 $\left\{p_1,p_2,\cdots,p_n\right\}$ 由属性组成。单调访问结构可以用与门和或门组成的单调布尔公式直观表达，通常使用单调张成方案转化为矩阵 M 与映射 ρ，其中 M 的第 i 行被属性 ρ_i 标记。设 S 为属性集合，若存在系数 $\left\{\omega_i\right\}_{\rho_i\in S}$，使得

$$\sum_i\omega_iM_i=\left(1,0,0,\cdots,0\right)$$

则称 S 满足访问结构 Υ。

2.3. 密文策略属性基加密(CP-ABE)

传统的密文策略属性基加密方案由以下四个基本算法组成：

1) 初始化算法 $Setup\left(\lambda,P\right)$：系统 CA 运行初始化算法，输入为隐式安全参数 λ 与属性集合 P，输出公共参数 PK，系统主密钥 MSK。

2) 加密算法 $Encrypt\left(PK,m,\Upsilon\left(M,\rho\right)\right)$：数据管理者运行加密算法，输入为公共参数 PK，欲加密明文 m 及访问结构 $\Upsilon\left(M,\rho\right)$，输出密文 CT。只有拥有满足访问结构的属性的数据请求者才能解密。

3) 密钥生成算法 $KeyGen(MK,S)$：系统 CA 运行密钥生成算法，输入为系统主密钥 MSK 与属性集合 S，该算法将属性集合与密钥关联，输出属性密钥 SK。

4) 解密算法 $Decrypt(PK,CT,SK)$ 数据请求者运行解密算法，输入为公共参数 PK，密文 CT 与属性密钥 SK，若与 SK 关联的属性集合满足 CT 所包含的访问结构 $\Upsilon(M,\rho)$，则该算法将解密 CT 输出明文 m。

2.4. Hyperledger Fabric

本方案所采用的区块链平台为 Hyperledger Fabric。Fabric 是一种使用模块化结构的许可链，其中具有决定性的扩展功能为智能合约(Smart Contract)。如图 1 所示，Fabric 与其他区块链平台最为显著的区别在于其模拟(simulation)、排序(ordering)、验证(validation)、提交(commit)的交易执行顺序：

1) 模拟：客户端发起交易请求，该请求被发送至经背书策略(endorsement policy)选择的背书节点(endorsement nodes)。背书节点模拟执行交易后形成读写集(ReadWriteSet)，并将读写集与背书签名发送回客户端。客户端收集到足够背书后，则生成真正的交易请求，该请求包含之前收到的读写集与背书签名，然后发送给排序服务。

2) 排序：排序服务按照交易到达顺序排序，然后将一定数量的交易打包形成块(block)，将块发送至网络中所有对等节点。系统不保证所有对等节点同时收到相同的块，但基于 gossip 协议保证所有对等节点收到块的顺序相同。

3) 验证：对等节点收到块后，即对块中包含的交易进行验证。一方面验证该交易是否遵循背书策略且包含的背书签名与读写集是否对应。另一方面为交易冲突验证：Fabric 模型中并行进行的模拟交易位于排序服务之前，可能会产生冲突。两方面验证都通过后，进入提交阶段。

4) 提交：对等节点将包含所有交易的块添加到区块链，并根据有效交易更新账本状态。

一个分布式 Fabric 应用包含两个主要组成部分：链码(Chaincode)、背书策略(Endorsement Policy)。

链码：在 Fabric 中智能合约又称为链码。链码是一种可以运行在区块链上实现特定交易逻辑的可编程应用。Fabric 拥有强大的容器技术来支持图灵完备语言编写的链码，例如：GoLang、Java、Node.Js。

背书策略：背书策略规定了必须执行特定交易并为之背书的节点，也可指定特定交易背书的最少节点、最小百分比等。一笔交易在被提交前，必须符合背书策略。

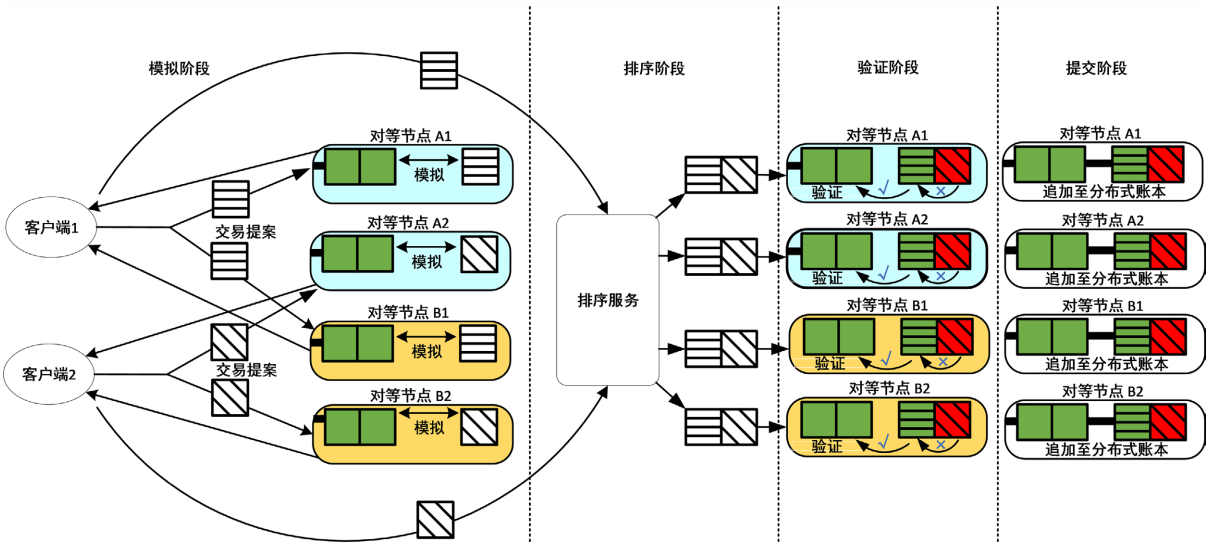

Figure 1. Hyperledger Fabric workflow
图 1. Hyperledger Fabric 工作流

3. 方案架构

本文所提出的基于区块链的轻量级访问控制方案架构如图 2 所示，主要由五部分组成，分别是：数据管理者(DM)、数据请求者(DR)、身份认证模块(CA)、区块链模块(Block Chain)、云服务器(Cloud Server)，各部分功能的具体描述如下：

身份认证模块主要负责对系统进行初始化和为数据请求者生成属性令牌；该部分默认可信。

数据管理者是数据资源(访问客体)的拥有者，主要负责对原始数据执行对称加密、存储数据密文至云服务器以及在区块链上部署相应的访问控制结构。

数据请求者是访问主体，主要负责发送数据访问请求至区块链、验证区块链的预解密结果、从云服务器下载数据密文进行解密。

区块链模块主要负责处理数据请求者与数据管理者的交易请求以及执行预解密操作。

云服务器负责存储、传输系统中产生的大规模数据密文。

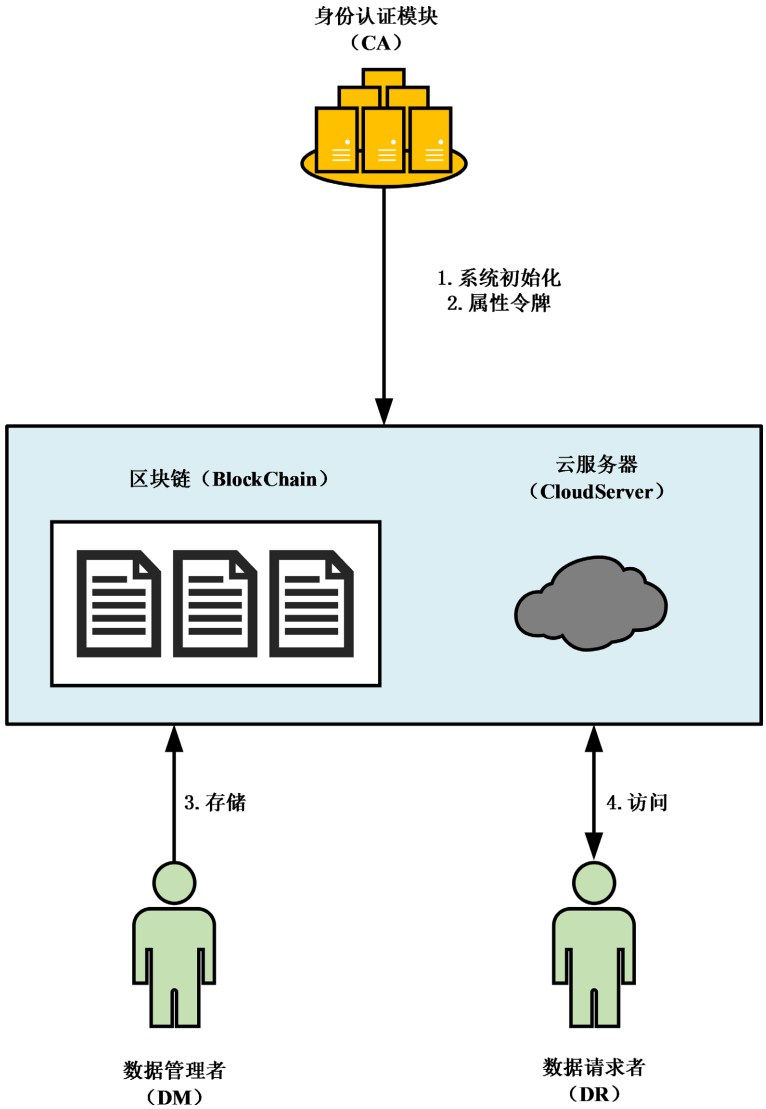

Figure 2. Access control scheme architecture
图 2. 访问控制方案架构图

如图 2 所示，CA 首先产生公共参数，然后将其上传至 Block Chain 来对系统进行初始化；当 DR 加入 Block Chain 时，CA 根据 DR 所包含的属性通过智能合约为其产生属性令牌并分发；DM 分别上传数据密文与属性密文至 Cloud Server 和 Block Chain；DR 发送访问请求至 Block Chain，预解密在 Block Chain 上执行，若属性匹配，则预解密成功；随后，DR 得到预解密结果与数据密文，执行最终解密。

4. 访问控制算法

本方案的访问控制算法分为六部分，分别是系统初始化、加密、属性令牌、预解密令牌、预解密、本地解密。

如图 3 所示，在初始化阶段，CA 生成公共参数 PK 和系统主密钥 MSK，公共参数上传至区块链公开，主密钥安全保存；在数据存储阶段，数据管理者先将明文 M 使用对称密钥 SK_M 加密后得到数据密文 M^*，然后对对称密钥 SK_M 进行属性加密得到属性密文 CT，最后将属性密文 CT 和数据密文 M^* 上传至云服务器与区块链；在数据访问阶段，数据请求者首先依据自身属性通过 CA 生成属性令牌 T_S，然后将属性令牌转化为预解密令牌 T_S^* 上传至区块链，区块链用该预解密令牌对属性密文执行预解密后将结果 CT^* 返回至数据请求者，数据请求者在本地执行最终解密，得到对称密钥 SK_M 并验证，最后，用该对称密钥解密从云服务器下载的数据密文得到明文，执行数据访问。以下是每部分的详细描述：

1) 系统初始化

CA 运行初始化算法 $Setup(\lambda,U)$，输入安全参数 λ 与属性集合 $U=\{1,2,\cdots,i\}$，生成公共参数 PK 与系统主密钥 MSK 来对系统进行初始化：

CA 运行算法 $\varphi(\lambda)$ 得到 (p,G,G_S,e)，其中 G 与 G_S 为 p 阶循环群；然后随机选择 $g,d,x,y\in G$，$\alpha,\beta\in Z_p^*$，对于属性集合 U 中的每一条属性 i，随机选择 $s_i\in Z_p^*$ 与之对应；最后选择哈希函数 $H:G\to Z_p^*$。则：

$$MSK=\alpha$$

$$PK=\left(G,G_S,e,g,d,x,y,e(g,g)^{\alpha},g^{\beta},H,T_i=g^{s_i}\ \forall i\in U\right)$$

2) 加密

DM 对数据资源 M 进行对称加密，得到数据密文 M^* 后将其存储至云服务器，然后输入公共参数 PK、对称密钥 SK_M、线性访问结构 $\Upsilon=(A,\rho)$ (A 为 $i\times n$ 阶矩阵，ρ 为矩阵 A 的行向量 A_i 向属性 ρ_i 的映射)，用加密算法 $Encrypt(PK,SK_m,\Upsilon)$ 来加密对称密钥 SK_M：

加密算法随机选择向量 $v,v^*\in Z_p^{*n}$ ($v=(s,v_2,\cdots,v_n)$，$v^*=(s^*,v_2^*,\cdots,v_n^*)$)，$SK_{M^*}\in G_S$；对于矩阵 A 的行向量 A_i，随机选择 $r_{1,i},r_{2,i}\in Z_p^*$。则：

属性密文 $CT=\left(\Upsilon,\bar{C},C_1,C_1^*,C_{1,i},D_{1,i},C_2,C_2^*,C_{2,i},D_{2,i}\right)$

其中：

$$\bar{C}=u^{H(SK_M)}v^{H\left(SK_{M^*}\right)}d$$

$$C_1=SK_M e(g,g)^{\alpha s},\ C_1^*=g^s,\ C_{1,i}=g^{\beta A_i\bar{v}},\ D_{1,i}=g^{r_{1,i}}\quad\forall i\in U$$

$$C_2=SK_{M^*}e(g,g)^{\alpha s^*},\ C_2^*=g^{s^*},\ C_{2,i}=g^{\beta A_i\overline{v^*}}T_{\rho(i)}^{-r_{2,i}},\ D_{2,i}=g^{r_{2,i}}\quad\forall i\in U$$

3) 属性令牌

CA 运行属性令牌算法 $TokenGen(PK,MSK,S)$ 为 DR 生成属性集合 S 所对应的令牌 T_S：

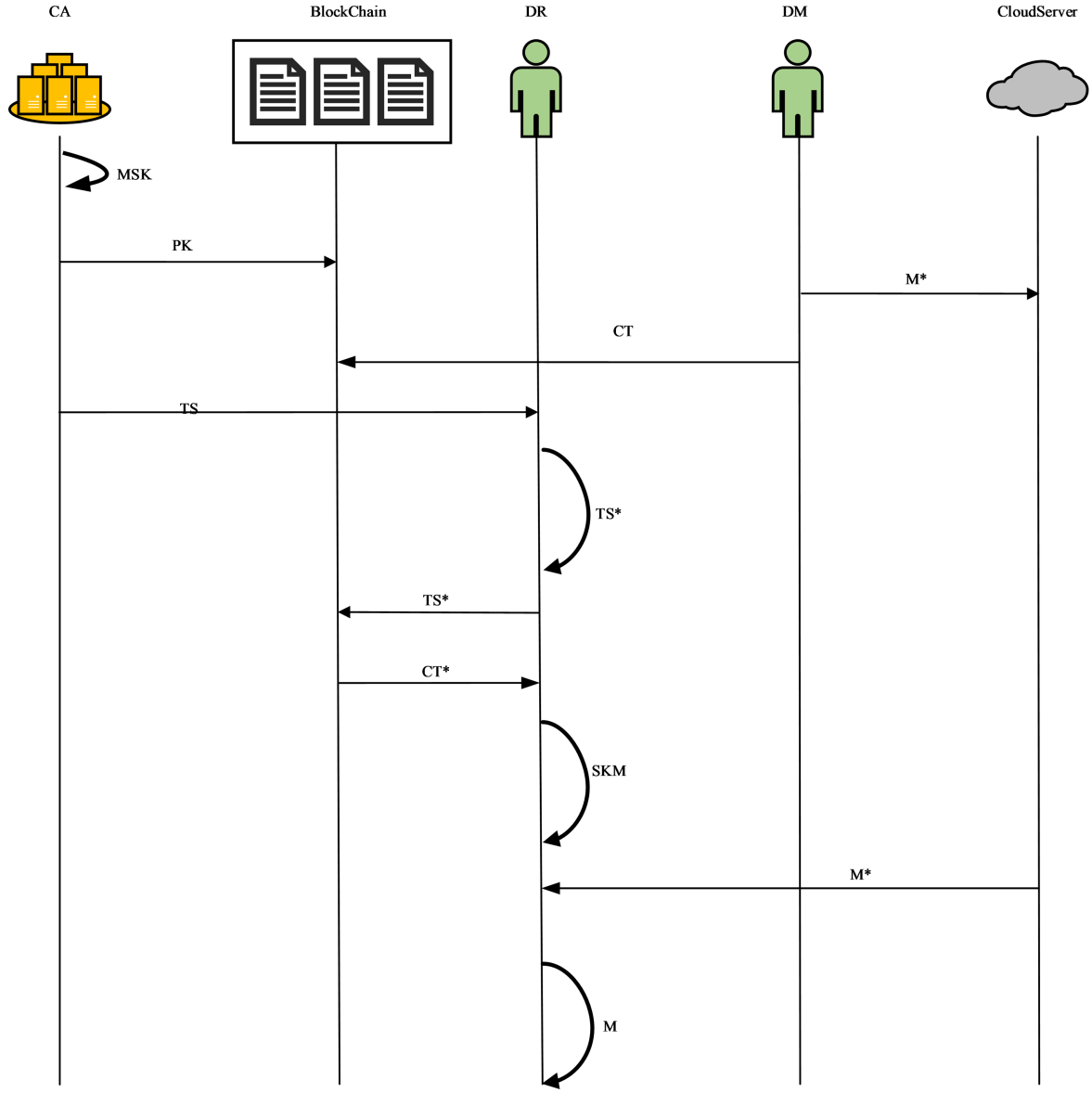

Figure 3. Access control algorithm
图 3. 访问控制算法

随机选择 $t \in Z_p^*$，则：

$$T_S = \left(S, K_0, K_1, K_i\right)$$

其中：

$$K_0 = g^{\alpha} g^{\beta t}$$

$$K_1 = g^t$$

$$K_i = T_i^t \quad \forall i \in S$$

4) 预解密令牌

DR 运行预解密令牌算法 $PreToken\left(PK, T_S\right)$ 生成预解密令牌 T_S^*：

随机选择 $z \in Z_p^*$，恢复密钥 $RK_S = z$，则：

$$T_S^* = \left(S, K^* = K^{1/z}, K_0^* = K_0^{1/z}, K_i^* = K_i^{1/z} \ \forall i \in S\right)$$

5) 预解密

区块链运行预解密算法 $PreDecrypt\left(PK, CT, T_S\right)$：

若属性令牌 T_S 中所包含的属性不能满足线性访问结构 Υ，则预解密失败，输出 $ERROR$；

若属性令牌 T_S 中所包含的属性满足线性访问结构 Υ，则 $I \in (1,2,\cdots,l)$ 定义为 $I = \{i : \rho(i) \in S\}$，则必存在 $\omega_i \in Z_p^*$，使 $\sum_{i \in I} \omega_i A_i = (1,0,\cdots,0)$，预解密算法计算以下内容：

$$T_1^* = \frac{e\left(C_1^*, K^*\right)}{\prod_{i \in I}\left(e\left(C_{1,i}, K_0^*\right) e\left(K_{\rho(i)}^*, D_{1,i}\right)\right)^{\omega_i}} = \frac{e(g,g)^{\alpha s/z} e(g,g)^{\beta ts/z}}{\prod_{i \in I} e(g,g)^{\beta t A_i \vec{v} \omega_i / z}} = e(g,g)^{\alpha s/z}$$

$$T_2^* = \frac{e\left(C_2^*, K^*\right)}{\prod_{i \in I}\left(e\left(C_{2,i}, K_0^*\right) e\left(K_{\rho(i)}^*, D_{2,i}\right)\right)^{\omega_i}} = \frac{e(g,g)^{\alpha s^*/z} e(g,g)^{\alpha t s^*/z}}{\prod_{i \in I} e(g,g)^{\beta t A_i \vec{v}^* \omega_i / z}} = e(g,g)^{\alpha s^*/z}$$

预解密密文为：

$$CT^* = \left(\bar{T} = \bar{C}, T_1 = C_1, T_1^*, T_2 = C_2, T_2^*\right)。$$

6) 本地解密

DR 运行本地解密算法 $Decrypt\left(PK, CT, CT^*, RK_S\right)$，计算：

$$SK_M = \frac{T_1}{T_1^{*z}}, \quad SK_{M^*} = \frac{T_2}{T_2^{*z}}$$

若 $\bar{T} = u^{H(SK_M)} v^{H\left(SK_{M^*}\right)} d$，则说明区块链上的预解密正确执行，然后从云服务器下载数据密文 M^*，用对称密钥 SK_M 解密数据密文后得到明文 M，最后执行数据访问。

5. 安全性分析

5.1. 预解密机密性

预解密的机密性基于离散对数问题。本文所提方案通过随机选择的恢复密钥 $RK_S = z$ 产生预解密令牌 T_S^*。因此，即使敌手从区块链处获得预解密令牌 T_S^* 和属性密文 CT，也不能在没有恢复密钥 RK_S 的情况下计算出 SK_M。所以，本文所提方案的预解密机密性得以保证。

5.2. 防篡改攻击

假设有少部分对等节点在短时间内受到攻击，敌手可以添加、删除、篡改存储在这些对等节点中的属性信息和数据访问记录。以单个恶意物联网设备为例，首先，通过在系统初始化阶段指定只有 CA 能产生属性令牌来防止恶意节点篡改属性信息；其次，当系统中的恶意节点试图篡改已有属性时，根据区块链的背书机制，必须有超过一半的节点被篡改。事实上，这是非常困难的，即敌手不可能通过破坏少数节点来篡改区块链上的数据。因此，本文所提方案可以防篡改攻击。

5.3. 抵抗合谋攻击

当多个恶意 DR 从区块链获得自己的属性令牌后，他们可能将其合并来解密自身属性权限外的文件。

为了抵抗恶意 DR 的合谋攻击，属性令牌由 CA 随机选择的参数 t 来产生，不同的 DR 所采用的随机参数 t 是不同的。这样，恶意 DR 不能通过相互联合属性令牌来获取更多权限。因此，本文所提方案可以抵抗合谋攻击。

6. 结束语

本文提出了一种基于区块链的物联网数据访问控制方案，将区块链与属性基加密结合，借助智能合约技术，将属性基加密中开销高的双线性配对操作外包至区块链中执行预解密，然后在本地验证区块链预解密的正确性，解决了属性基加密应用于物联网资源受限设备中开销高的问题，从而减轻了用户端的计算压力，实现了轻量级的访问控制。安全分析结果表明，该方案在数据机密性、防篡改攻击和抵抗合谋攻击方面是可靠的。

参考文献

[1] Nakamoto, S. (2008) Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf

[2] Zheng, Z., Xie, S., Dai, H., Chen, X. and Wang, H. (2017) An Overview of Blockchain Technology: Architecture, Consensus and Future Trends. 2017 *IEEE International Congress on Big Data*, Honolulu, 25-30 June 2017, 557-564. https://doi.org/10.1109/BigDataCongress.2017.85

[3] Wang, Q., Zhu, X.Q., Ni, Y.Y., Gu, L. and Zhu, H.B. (2010) Blockchain for the IoT and Industrial IoT: A Review. *Internet of Things*, **10**, Article No. 100081. https://doi.org/10.1016/j.iot.2019.100081

[4] Sharma, A., Schuhknecht, F.M., Agrawal, D. and Dittrich, J. (2019) Blurring the Lines between Blockchains and Database Systems: The Case of Hyperledger Fabric. *Proceedings of the* 2019 *International Conference on Management of Data* (*SIGMOD*'19), 105-122. https://doi.org/10.1145/3299869.3319883

[5] Androulaki, E., Barger, A., Bortnikov, V., *et al*. (2018) Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains. *Proceedings of the Thirteenth EuroSys Conference* (*EuroSys*'18), 1-15. https://doi.org/10.1145/3190508.3190538

[6] Zyskind, G., Nathan, O., *et al*. (2015) Decentralizing Privacy: Using Blockchain to Protect Personal Data. 2015 *IEEE Security and Privacy Workshops*, San Jose, 21-22 May 2015, 180-184. https://doi.org/10.1109/SPW.2015.27

[7] Shafagh, H., Burkhalter, L., Hithnawi, A. and Duquennoy, S. (2017) Towards Blockchain-Based Auditable Storage and Sharing of IoT Data. 2017 *on Cloud Computing Security Workshop*, 45-50. https://doi.org/10.1145/3140649.3140656

[8] Ouaddah, A., Elkalam, A.A. and Ouahman, A.A. (2017) FairAccess: A New Blockchain-Based Access Control Framework for the Internet of Things. *Security and Communication Networks*, **9**, 5943-5964. https://doi.org/10.1002/sec.1748

[9] Zhang, Y., Kasahara, S., Shen, Y., Jiang, X. and Wan, J. (2019) Smart Contract-Based Access Control for the Internet of Things. *IEEE Internet of Things Journal*, **6**, 1594-1605. https://doi.org/10.1109/JIOT.2018.2847705

[10] Liu, H., Han, D. and Li, D. (2020) Fabric-iot: A Blockchain-Based Access Control System in IoT. *IEEE Access*, **8**, 18207-18218. https://doi.org/10.1109/ACCESS.2020.2968492

[11] Ding, S., Cao, J., Li, C., Fan, K. and Li, H. (2019) A Novel Attribute-Based Access Control Scheme Using Blockchain for IoT. *IEEE Access*, **7**, 38431-38441. https://doi.org/10.1109/ACCESS.2019.2905846

[12] Sahai, A. and Waters, B. (2005) Fuzzy Identity-Based Encryption. In: Cramer, R., Ed., *Advances in Cryptology—EUROCRYPT* 2005, Vol. 3494, Springer, Berlin, Heidelberg, 457-473. https://doi.org/10.1007/11426639_27

[13] Bethencourt, J., Sahai, A. and Waters, B. (2007) Ciphertext-Policy Attribute-Based Encryption. 2007 *IEEE Symposium on Security and Privacy* (*SP*'07), Berkeley, 20-23 May 2007, 321-334. https://doi.org/10.1109/SP.2007.11