doi: 10.7690/bgzdh.2025.06.010

# 基于区块链技术的智能油田信息安全防护建模

王利君，段　非，王白羽，王　婷
（新疆油田公司数智技术公司，新疆 克拉玛依 834000）

**摘要：**为保障智能油田信息的安全性，提出基于区块链技术的智能油田信息安全防护方法。对智能油田信息实施合理聚类后，构建不同种类智能油田信息数据集，使用基于主动学习的数据清洗技术，清洗各智能油田信息数据集；使用基于区块链与人工智能技术的数据加密传输方法，加密传输智能油田信息，并将其放入区块链实施分布式存储；信息访问者需获得认证凭证，方能合理访问智能油田信息。结果表明：将该方法应用于智能油田信息安全防护工作中，可显著提升智能油田信息的安全性，使其避免遭受网络攻击与非法访问。

**关键词：**区块链技术；智能油田信息；安全防护；数据清洗；数据加密；加密传输
**中图分类号：**TP309　　**文献标志码：**A

# Information Security Protection Modeling of Intelligent Oilfield Based on Blockchain Technology

Wang Lijun, Duan Fei, Wang Baiyu, Wang Ting
(*Xinjiang Oilfield Company Digital Intelligence Technology Co*., *Ltd*., *Karamay* 834000, *China*)

**Abstract:** In order to protect the information security of intelligent oilfield, the information security protection method of intelligent oilfield based on blockchain technology is proposed. Aft that intelligent oilfield information is subjected to reasonable cluster, different kinds of intelligent oilfield information data sets are constructed, the intelligent oilfield information data set are cleaned by using a data cleaning technology based on active learning, the intelligent oilfield information is encrypted and transmitted by using a data encryption transmission method based on a blockchain and an artificial intelligence technology, and the intelligent oilfield information is put into a blockchain for distributed storage; Information visitors need to obtain authentication certificates before they can reasonably access intelligent oilfield information. The results show that the application of this method in the information security protection of intelligent oilfield can significantly improve the security of intelligent oilfield information and avoid network attacks and illegal access.

**Keywords:** blockchain technology; intelligent oilfield information; security protection; data cleaning; data encryption; encrypted transmission

## 0　引言

数字化技术的不断发展，在很大程度上推动了智能油田的合理建设以及应用，也使得网络以及信息系统在智能油田建设以及应用工作中的作用不断增强[1-3]。当前，国内外网络所呈现出的安全形势很严峻，一些恶意分子或黑客组织，能够利用网络渗透以及网络攻击等方式窃取智能油田信息，这无疑给智能油田信息的安全性带来了极大威胁。此外，一些智能油田信息非法访问者对智能油田信息的非法访问在一定程度上也增加了智能油田信息泄露的概率。为充分保障智能油田信息安全，促进油田业务不断向高质量的方向发展，研究一种有效的智能油田信息安全防护方法，迫在眉睫。

近年来，国内外诸多学者研究了大量行之有效的智能油田信息安全防护方法：陈小娟等[4]研究的基于数据消冗技术的智能油田信息安全防护方法；韩培义等[5]设计的面向云存储的智能油田信息安全防护系统。前者通过 Bloom 过滤技术对智能油田信息执行合理降维操作，并使用 hash 函数求解智能油田信息在实施合理消冗时的误判率，之后以映射位数组为可靠依据明确最优扩列函数存在的数量，最终通过改进 ABE 加密方案加密智能油田信息，保障智能油田信息安全；后者设计一种有效的智能油田信息安全防护系统，使用 Java Script 动态程序分析技术，为智能油田信息自动识别以及适配相应云应用，对各云应用智能油田敏感信息执行合理加密保护工作，并对密文执行搜索功能集成操作，在对智能油田信息实施有效加密保护的同时，尽量保持了云应用的原始功能。二者均可实现智能油田信息安

**收稿日期：**2024-08-12；**修回日期：**2024-09-25
**第一作者：**王利君(1987—)，女，河南人，硕士。

全防护，但在智能油田信息安全防护工作方面还存在一定欠缺，安全防护效果距理想状态还存在一定差距。

区块链技术在数据安全防护领域，具有极其强大的安全防护性能，其本身便可被看成一个安全系数较高的数据库，将其应用于实际的智能油田信息安全防护工作中，可显著提升智能油田信息的安全性。笔者基于区块链技术对智能油田信息安全防护方法进行建模研究，以更好满足实际工作需要。

## 1 智能油田信息安全防护建模研究

### 1.1 智能油田信息安全防护模型构建

区块链实际上相当于一个共享性质的数据库，存储于其中的各数据拥有不可伪造以及全程留痕迹等特点，这使得区块链在实际工作中，能够利用其强大的安全防护性能，为各种数据信息搭建出一个安全系数极高的存储环境。区块链技术以应用、共识以及数据集合等部分为主要构成，其技术架构如图 1 所示。

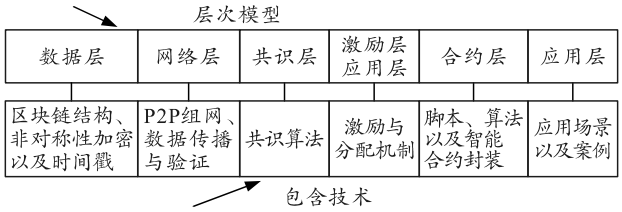


图 1 区块链技术架构

数据层、网络层以及共识层是该项技术的核心部分，其能够保障区块链技术在网络环境中的正常可靠运转，也是数据安全防护工作的关键。

鉴于区块链技术在数据信息安全防护方面的优势，笔者基于区块链技术构建智能油田信息安全防护模型，将智能油田信息放入区块链进行存储，并使用区块链与人工智能技术完成智能油田信息加密传输，构建的智能油田信息安全防护模型架构如图 2 所示。

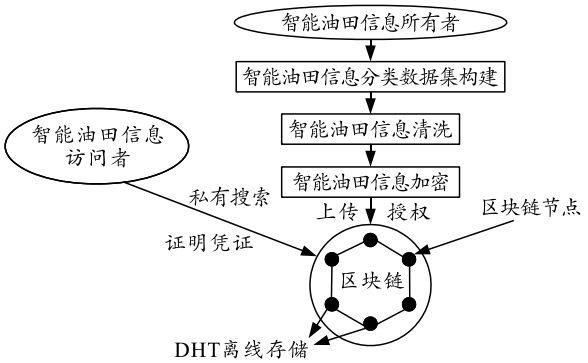


图 2 智能油田信息安全防护模型架构

智能油田信息所有者掌握智能油田信息，希望在满足实际工作需求前提下，尽量节省信息存储空间并保障智能油田信息的安全性，同时具备对智能油田信息访问者授权搜索的能力。在实际的工作中，智能油田信息所有者首先会对智能油田信息执行聚类操作，将所有的智能油田信息按一定的特征为标准分类成不同的智能油田信息数据集；然后对获得的各智能油田信息数据集实施有效的数据清洗操作，以去除智能油田信息中的冗余重复信息以及一些噪声干扰数据，并使数据在一定程度上具有一致性；完成相应的数据清洗操作后，使用基于区块链的加密技术对其实施合理加密，并放入区块链中进行分布式存储，对智能油田信息实施有效的安全防护，使智能油田信息避免遭受网络中的恶意攻击，并有效制止非授权访问客户的非法访问行为，保障智能油田信息的安全性。智能油田信息访问者是智能油田信息所有者的授权客户，若智能油田信息访问者已经得到智能油田所有者授予的访问权限，那么可以和区块链节点实施合理交互操作，证明其访问权限，并对智能油田信息执行相应的搜索工作。区块链节点在整个模型中，能够对整个区块链实体起到合理维护的作用，在智能油田信息安全防护工作中发挥着非常关键的作用。

智能油田信息安全防护模型中所使用的区块链技术以比特币底层为主要来源，应用于智能油田信息安全防护工作中，可显著提升智能油田信息防护的效果。区块链实质上是由块构成的，然后以哈希指针为连接媒介按一定的顺序被连接成一个整体，因哈希函数本身具备强大的加密性能，故将数据应用加密技术放入区块链中实施存储后，会具有更强大的安全防护功能，更能有效保障智能油田信息的安全性。

DHT 标记的是分布式哈希表，在实际的工作中区块链存储的是对智能油田信息的应用，而非智能油田信息本身。模型充分考虑了区块链在运行时的场景，无论在模型性能还是在安全性方面，较以往在智能油田信息安全防护工作中构建的无权限智能油田信息安全防护模型，在智能油田信息防护工作中都具有显著优势。为对智能油田信息安全防护流程进行更加真实化说明，给出如下智能油田安全防护事例。

智能油田信息所有者 $C$ 为保障所掌握智能油田信息安全，在将其拥有的智能油田信息上传至云之

前，对其执行有效聚类操作，将其分类成不同数据集，并对所获数据集进行数据清洗，获得更为精准的智能油田信息，然后在客户端使用基于区块链的加密技术对各数据集实施合理加密，并为其添加相应的关键字标签。完成加密的智能油田信息数据集最终由云联盟对其实施分布式存储，加密的关键字标签由区块链实施相应维护，用于完成索引以及访问相匹配的智能油田信息加密文档。

上述工作完成后，智能油田信息所有者 $C$ 能够授权智能油田信息访问者 $D$，在智能油田信息加密数据集上执行相应搜索操作的权限；此时，智能油田信息访问者 $D$ 可以向区块链节点证明其拥有执行智能油田信息搜索的权利。由于在实际的工作中会存在多个智能油田信息访问者，因而凭证或证明应是以匿名形式存在的，以保证智能油田信息访问者的隐私，换言之就是模型的区块链中，智能油田信息访问者 $D$ 是众多智能油田信息访问者中的一个，但是无法对其隐私身份执行提取操作；同时，区块链节点，也不能够确定某个凭证或证明是否由一人构建。智能油田信息访问者 $D$ 不能下载整个智能油田信息数据集，而是需要根据搜索的关键字在联合云中对所需数据集执行必要的检索操作。

### 1.2　基于主动学习的智能油田信息清洗

为有效提升智能油田信息安全防护工作的效率，并在区块链中获得更多的智能油田信息存储空间，在运用区块链技术完成智能油田信息加密工作之前，智能油田信息所有者首先应使用合理的技术手段对智能油田信息实施合理的数据聚类，将其划分为不同种类的智能油田信息数据集，然后对各数据集实施有效的数据清洗，究其原因主要是对数据实施有效的数据清洗操作，可有效去除数据中存在的噪声数据、无关数据、空值数据以及填补一些缺失数据[6-8]，从而保障数据的质量。

笔者使用基于主动学习的数据清洗技术对智能油田信息执行有效的清洗操作，基于主动学习的数据清洗技术架构如图 3 所示。

在该技术架构中，数据存储部分的主要职责是负责准备智能油田信息，对智能油田信息执行合理的初步处理操作后，将其向数据学习部分传递，在数据方面给予确定度模型可靠数据支撑[9-10]；数据学习部分的主要职责是维护以及运行确定度模型，并为数据选择部分提供一系列由确定度模型建议修复的智能油田数据，通常这些建议修复的智能油田信息会附带相应的确定度值，用以表示该智能油田信息确定修复的程度[11]；数据选择部分所承担的职责是实施智能油田数据修复选择以及人机交互操作，利用相应的数据运行筛选规则，挑选出由确定度模型建议的最容易出现错误的修复数据给智能油田信息所有者查看，然后由智能油田所有者确认该智能油田信息是应该被划分为干净智能油田信息还是待清洗智能油田信息，并将其向数据存储部分反馈，对干净的智能油田信息数据训练集执行有效的扩充操作，如此反复迭代增强确定度模型的学习性能，最终经无数次迭代操作后，完成相应的智能油田信息清洗工作。

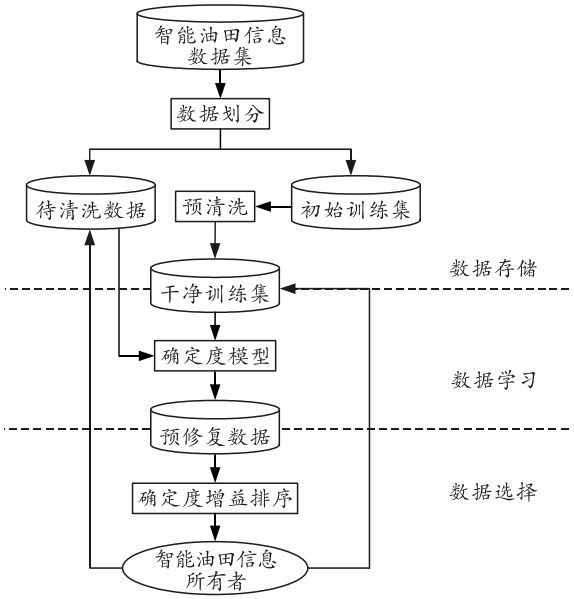


图 3　主动学习数据清洗技术架构

### 1.3　智能油田信息加密

使用传统的加密方式，往往只能保障单个数据集在存储与共享时的安全性，一旦需要保障的数据集较多，便无法更好满足实际工作需要[12-13]。鉴于区块链技术与人工智能技术在数据安全防护方面的优势，笔者使用基于区块链与人工智能技术的数据加密算法对智能油田信息数据集实施有效加密，保障其安全性。

在对智能油田信息各数据集实施有效加密时，将智能油田信息按时间顺序分解成不存在任何关系的智能油田信息，并将其按一定标准顺序构建成链式信息结构，用加密存储的方式对分解完成的智能油田信息实施分布式存储。具体的加密流程为：

对智能油田信息源节点 $F$ 执行合理的分解操作，将其分解成份数为 $m$ 的智能油田信息，并将其标记为 $k_1$，$k_2$，…，$k_m$，之后将其传输至目标节点，

在对该信息实施合理传输前，$F$ 会相应地产生数量为 $r$、维度为 $m$ 的智能油田信息向量，并且每个智能油田信息向量又拥有数量为 $m$ 的小分量，将这些小分量用公式标记为 $d_1$, $d_2$, …, $d_r$，可得到相应的加密公式，具体可描述成：

$$\left.\begin{array}{l} d=(d_{i1}, d_{i2}, \cdots, d_{im}) \\ i=1, 2, \cdots, r \end{array}\right\}。 \tag{1}$$

将执行过信息编码处理操作的矩阵用公式进行相应描述，有：

$$\begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_r \end{bmatrix} = \begin{bmatrix} d_{11}, d_{12}, \cdots, d_{1m} \\ d_{21}, d_{22}, \cdots, d_{2m} \\ \vdots \quad \vdots \quad \quad \vdots \\ d_{r1}, d_{r2}, \cdots, d_{rm} \end{bmatrix} \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_m \end{bmatrix}。 \tag{2}$$

将数量为 $r$、维度为 $m$ 的智能油田信息向量向式(2)实施有效的代入，执行有效的编码计算操作，用 $t$ 标记时间，在 $t$ 段内，将执行过应编码处理操作的 $r$ 个智能油田信息数据包标记为 $b_1$, $b_2$, …, $b_r$，可将其求解过程描述为：

$$b_1, b_2, \cdots, b_r=(d_1, d_2, \cdots, d_r)\times(a_1, a_2, \cdots, a_m)^t。 \tag{3}$$

式中 $a_1$, $a_2$, …, $a_m$ 为原始智能油田信息数据包。

对 $F$ 完成相关编码操作的智能油田数以及与其相对应的智能油田信息编码向量执行有效统一的打包处理操作，从而得到数量为 $r$ 的智能油田编码信息数据包，并将所获智能油田编码信息数据包向目标节点传输。目标节点获得这些数据包后，由于对其实施合理编码处理，所获的向量信息不具备线性特征，故可得到原始智能油田信息数据矩阵，用公式可描述为：

$$\begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_m \end{bmatrix} = \begin{bmatrix} d_{11}, d_{12}, \cdots, d_{1m} \\ d_{21}, d_{22}, \cdots, d_{2m} \\ \vdots \quad \vdots \quad \quad \vdots \\ d_{r1}, d_{r2}, \cdots, d_{rm} \end{bmatrix} \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_r \end{bmatrix}。 \tag{4}$$

以式(4)为可靠依据，对密钥用户存储的初始指纹实施合理选择，通常状况下，该指纹以数量为 512 的字节为主要构成[14-15]，对密钥存储者来说安全系数是比较高的，在加密环境安全系数较高的情况下，对智能油田信息的加密执行过程应用区块链以及人工智能技术实施合理设计，具体的过程可归结如下：

1) 智能油田信息所有者选择相应的智能油田信息文件。

2) 实施合理的指纹身份识别操作。

3) 确定该用户身份是否为新注册用户，若是，将其作为首个指纹模板；反之，说明程序出现异常状况，不能执行加密操作，需要重新选择智能油田信息文件。

4) 按式(1)—(4)对智能油田信息文件执行合理加密操作。

5) 询问是否将智能油田信息的源文件删除，若是，直接删除；否则，证明程序无异常状况，能够直接完成相关加密处理操作。

在完成相应的智能油田信息加密工作后，使用人工智能中包含的移动 agent 完成智能油田信息加密传输。由主 agent 在相应的本地设备中生成一对密钥，分别用作执行加密操作的公开密匙与执行解密操作的私有密匙。由子 agent 负责将前者带至远程设备，用于执行智能油田信息加密操作，并由主 agent 负责保管后者，将其存储于本地设备中，不让其在网络中进行传递。子 agent 完成相关任务后，将智能油田信息加密文件发送给主 agent，主 agent 在接收到由子 agent 传输过来的智能油田信息加密文件后，可使用解密密匙获取明文，完成一次智能油田信息的安全可靠传输。在整个加密传输过程中，即使智能油田信息被截获也无法被破译，极大地保障了智能油田信息在数据传输过程中的安全。

## 2 实验与分析

以河北地区的某智能油田为实验对象，应用本文中方法对该智能油田实施合理的智能油田信息安全防护，验证本文中方法有效性。据悉，该智能油田于 2020 年 5 月建成投用，在实际工作中使用云计算、人工智能以及大数据等先进的信息技术手段对传统油田执行有效赋能操作，完成了 150 余组的智能算法模型构建工作，并使用有效手段编写了代码约 140 多万行，与此同时，还完成了相应的流程再造工作，是一个集现代智能以及数字化技术于一身的新型智能油田。

实验中搭建的区块链数据库，包含 6 个节点，分别将其用字母标记为 $A$、$B$、$C$、$D$、$E$ 与 $F$，其中：$A$、$B$、$C$、$D$、$E$ 作为区块链数据库智能油田信息存储结节存在，为重量级别的智能油田信息所有者以及区块链使用人员；$F$ 是级别较轻的智能油田信息所有者以及区块链使用人员，不具备数据存储功能，所拥有的数据有且只能存储于区块链数据库中；节点 $A$ 是区块链模型中的主节点。

实验中，将 6 个智能油田信息所有者在工作过程中产生的智能油田工作文件，当作智能油田信息，

对其进行加密传输，放入区块链数据库实施合理存储，完成智能油田信息安全防护，各智能油田工作文件关键词由智能油田信息所有者产生。

为验证本文中方法在智能油田信息安全防护工作中的有效性，在诸多油田信息所有者所拥有的文件中最终挑选一份有关 F0021 号油井设计参数的文件，对其实施加密传输，并在文件传输的过程中由实验测试人员在网络中加入一种非常严重的网络攻击病毒对加密文件进行攻击。表 1 为关于 F0021 号油井设计参数的原文件内容，表 2 为由实验测试人员在网络中加入攻击病毒后窃取到的 F0021 号油井设计参数信息状况。

**表 1　F0021 号油井设计参数**

| 参数名称 | 参数值 | 参数名称 | 参数值 |
|---|---|---|---|
| 外径范围/英寸 | 4.2 | 主体压力等级/psi | 11 000 |
| 最高流量/(桶/日) | 28 000 | 最高设计温度/(°F) | 300 |
| 最大长度/英尺 | 20.93 | 最高操作温度/(°F) | 240 |

**表 2　窃取到的 F0021 号油井设计参数**

| æ¯”è¾ƒè¾ | “å…¥ç§„édu |
|---|---|
| Œè¯ ç å | Œå®žé™… |
| çŸæ^ çš„éªŒè¯ | ç æ˜¯å ¦ç›¸åç¦ |
| å»ºå®½½å®¢æ | èµ„æ––å»ºå |
| fé›†å›¢Šæµ·d | æµ·å»ºå ^æŠ• |
| ç®¡ç †æœ‰é | £ä»»å…¬å |
| è šèµ„æœ¬å† | é¡¶èµ„æœ |

分析表 1 与 2 可知，在网路中加入攻击后，窃取到的 F0021 号油井设计参数信息，全部显示成乱码。证明在应用本文中方法对智能油田信息实施安全防护后，即使智能油田信息被攻击截获，也无法窃取到智能油田信息的真实内容，验证了本文中方法的有效性。

图 4 为智能油田信息访问者访问某个智能油田信息时，弹出的智能油田信息访问认证界面。

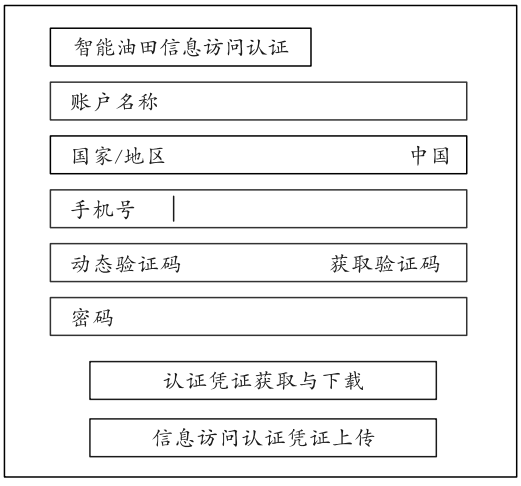


**图 4　智能油田信息访问认证界面**

从图 4 可以看出：当智能油田信息访问者想要访问某个智能油田信息时，需要获取下载并上传相应的信息访问认证凭证，才能够获取到智能油田信息的访问权限。由此可见，本文中方法不仅可有效防护网络中存在的攻击行为对智能油田信息安全的威胁，而且可有效限制实际工作中的一些智能油田信息非法访问行为，在智能油田信息安全防护方面优势显著。将本文中方法应用于智能油田信息安全防护工作中，可收获较为理想的智能油田信息安全防护效果。

进行多个智能油田信息加密传输时，在加密传输过程中，如果信息被全部置乱，则在传输过程中更具安全性，不容易被窃取或丢失。图 5 显示的应用本文中方法对智能油田信息所有者 *A* 拥有的 6 个智能油田工作文件实施加密传输，获得的信息置乱效果，其中，编号 $U_1$、$U_2$、$U_3$、$U_4$、$U_5$、$U_6$ 分别对应 6 个智能油田工作文件。

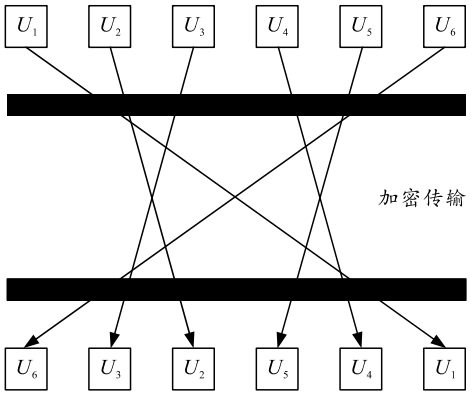


**图 5　加密传输置乱效果**

从图 5 可以看出：应用本文中方法对智能油田信息实施加密传输，传输过程中智能油田工作文件的顺序已经全部被置乱，更利于保障智能油田信息安全。证明本文中方法在智能油田信息安全防护方面较具优势，可更好满足实际工作需要。

## 3　结论

应用本文中方法可较好完成智能油田信息安全防护工作，保障智能油田信息安全；但是，在试验中仅加入了一种非常严重的攻击，对智能油田信息安全防护的效果进行验证。在实际工作中，网络中出现的攻击行为可能有很多种，为使本文中方法在智能油田信息安全防护工作中具有更为普遍的适用性，下一阶段，将从该角度出发对智能油田信息安全防护方法作进一步研究。

（下转第 73 页）