doi:10.6041/j.issn.1000-1298.2025.05.056

牡蛎供应链生物风险因子溯源隐私数据加密共享方法研究

孙传恒[1,2]　张　军[1,2]　罗　娜[2,3]　徐大明[2,3]　陈　枫[2,3]　邢　斌[2,3]

(1. 上海海洋大学信息学院, 上海 201306; 2. 农产品质量安全追溯技术及应用国家工程研究中心, 北京 100097;
3. 国家农业信息化工程技术研究中心, 北京 100097)

摘要: 牡蛎农产品在市场流通过程中可能携带传带性病毒、细菌等生物风险因子,已在多个国家引发频繁的生物安全事件。生物风险检测数据具有显著的隐私性特点,风险检测信息的不当泄露会造成公共卫生安全威胁。提出了一种基于区块链的牡蛎供应链生物风险因子隐私数据加密共享方法,通过对供应链中各个环节生物风险因子检测的数据进行加密上链存储,保证数据安全共享,风险源头可追溯。该方法基于属性的可搜索加密算法对生物风险因子检测数据进行访问控制和隐私保护,并构建加密倒排索引进行查询效率的优化,通过可搜索加密算法和倒排索引的结合实现快速定位到相关风险批次货物的详细数据。实验测试结果表明,生物风险检测数据关键词的加密时间平均为 31 ms,陷门生成时间平均为 32 ms,可搜索密文与陷门的匹配时间平均为 16 ms。监管者通过密文倒排索引查询风险牡蛎农产品相关数据的平均时间为 385 ms,并基于以太坊区块链平台构建了原型系统,实现生物风险因子密文隐私数据上链存储和追溯查询等功能,结果表明该方法能够满足牡蛎供应链隐私数据共享场景需求,为牡蛎生物风险监管提供技术支撑。

关键词: 区块链; 生物风险因子; 溯源; 可搜索加密; 倒排索引

中图分类号: TP311.11　　**文献标识码**: A　　**文章编号**: 1000-1298(2025)05-0577-12　　**OSID**:

Research on Method of Encrypted Sharing of Privacy Data for Tracing Biological Risk Factors in Oyster Supply Chain

SUN Chuanheng[1,2]　ZHANG Jun[1,2]　LUO Na[2,3]　XU Daming[2,3]　CHEN Feng[2,3]　XING Bin[2,3]

(1. *College of Information Technology, Shanghai Ocean University, Shanghai* 201306, *China*
2. *National Engineering Research Center of Agricultural Product Quality and Safety Traceability Technology and Application, Beijing* 100097, *China*
3. *National Engineering Research Center for Information Technology in Agriculture, Beijing* 100097, *China*)

Abstract: Oyster agricultural products may carry transmissible viruses, bacteria, and other biological risk factors during their market circulation, which has caused frequent biosecurity incidents in many countries and seriously threatened people's health. The privacy characteristics of biological risk detection data are significant, and the improper disclosure of biological risk detection information can pose a threat to public health security. A privacy-preserving data encryption and sharing method for oyster supply chain biological risk factors was proposed based on blockchain technology. By encrypting and storing biological risk factor detection data from various links in the supply chain on the blockchain, data security and sharing were ensured, and the source of the risk can be traced back. The method used attribute-based searchable encryption algorithms to perform access control and privacy protection on biological risk factor detection data, and an encrypted inverted index for query efficiency optimization was constructed. By combining searchable encryption algorithms and inverted indices, rapid location of relevant risk batch goods' detailed data was achieved. The experimental test results showed that the average encryption time of biological risk detection data keyword was 31 ms, the average trapdoor generation time was 32 ms, and the average matching time of searchable ciphertext and trapdoor was 16 ms. The average time for regulators to query risk oyster agricultural product-related data through encrypted inverted index was 385 ms, and a prototype system was built on the Ethereum blockchain platform to realize the functions of biological risk factor encrypted privacy data storage and traceability query. The results showed that the method can meet the demand of privacy data sharing scenarios in oyster supply chain and provide technical support for oyster biological risk regulation.

Key words: blockchain; biological risk factors; traceability; searchable encryption; inverted index

收稿日期: 2024-12-26　修回日期: 2025-01-17

基金项目: 国家重点研发计划项目(2023YFF0614404)和江苏省科技计划(重点研发计划现代农业)项目(BE2023315)

作者简介: 孙传恒(1978—),男,研究员,主要从事区块链技术研究,E-mail: sunch@nercita.org.cn

通信作者: 邢斌(1991—),男,副研究员,主要从事区块链技术研究,E-mail: xingb@nercita.org.cn

0 引言

牡蛎(Ostrea)是全球第一大养殖贝类,我国作为世界上最大的牡蛎养殖国之一,其产量占据了养殖贝类的80%左右[1-3]。牡蛎的滤食特性使其容易从环境中富集致病菌、病毒和微生物等,尤其是当消费者偏好生食牡蛎时,这些潜在的健康风险被显著放大,从而对食品安全构成了严重威胁[4-7]。

牡蛎供应链是一个全面覆盖从养殖、加工到销售等各个环节的复杂系统。在整个供应链中,食品安全问题始终是核心关注点。为了保护消费者健康,加强牡蛎供应链中生物风险因子数据的监管尤为重要[8-9]。但是,传统的农产品供应链的数据管理存在一些弊端,由于数据的中心化存储,存在数据孤岛、透明度不足、追溯性差等问题[10-11],导致无法及时发现并控制潜在的有害风险因子,增加了有害物质超标或病原体传播的可能性,直接威胁到消费者的健康安全。使用区块链技术,不仅可以提高牡蛎供应链中数据的透明度和可追溯性,还能够确保只有授权的参与者才能访问敏感数据[12-13]。此外,传统的牡蛎供应链数据通常以明文形式在供应链各环节间传递,这不仅增加了隐私数据泄露的风险,而且一旦生物风险因子检测数据被不当公开,可能会给企业带来声誉损失,甚至引发舆情风险[14]。

国内外研究人员对农产品区块链的隐私数据保护以及数据的访问控制展开了广泛的研究[15-19]。尽管加密算法对农产品的隐私数据保护方面取得了显著成果,但会导致隐私数据的密文无法进行有效的检索[20-21]。这给监管者对生物风险因子检测数据的审查带来了挑战,使得生物风险因子的追溯变得困难。为了使得隐私数据在密文的情况下可搜索,学者们做了一系列研究[22-26]。这些方案通过集成可搜索加密算法和倒排索引技术,实现了加密数据的可检索性,并利用相关索引结构优化了查询效率。

本文针对牡蛎农产品供应链的特性,提出基于区块链的牡蛎供应链生物风险因子隐私数据加密共享方法。通过基于属性的可搜索加密算法,允许检疫机构精确控制对生物风险检测数据的访问权限,确保只有监管者和获得授权的企业才能够查看敏感的检测信息,并通过在链下构建改进的密文倒排索引,提高密文的检索效率,以便及时发现和处理潜在的食品安全问题,减少生物风险传播。

1 牡蛎供应链关键信息分析和区块链模型架构

1.1 牡蛎供应链中溯源数据分析

在牡蛎供应链中,生物风险因子数据呈现出多源异构的特性,涵盖了生产养殖、加工分级、储存保鲜、物流运输以及批发销售等多个环节[27]。这些环节中可能隐藏着对牡蛎安全和质量以及对消费者食品健康安全构成威胁的病原体和病毒等生物风险因子[28]。然而,这种复杂性使得识别并追溯高风险传染性生物因子的具体来源变得困难。因此,将每个环节的数据分为公开溯源数据和生物风险隐私数据[29-31]。公开溯源数据主要用于提供给消费者查询,以明文形式存储,可以不受限制地共享和访问,用于基本的牡蛎产品信息查询,不涉及敏感的个人或企业信息。生物风险隐私数据则是指对牡蛎某一批次进行生物风险抽样检测数据,由于这类数据的公开可能引发社会舆情风险,因此需要进行隐私保护。通过访问控制,使这些隐私数据仅限于监管部门和相应的被授权主体企业查看,普通消费者无法查询。生物风险因子数据和货物信息公开溯源数据一并记录在区块链上。一旦检疫机构在数据上传过程中发现在供应链某一个环节中包含高危生物风险检测数据,系统即刻将该批次货物的公开溯源数据和生物风险隐私数据通报给监管部门和相关企业,各环节的关键溯源信息如表1所示。在深入分析牡蛎供应链中数据特点的基础上,以养殖环节为例,链上的隐私数据是生物风险因子检测报告数据密文哈希值,公开溯源数据则是牡蛎农产品在供应链中的流转详细信息,链上的公开追溯数据和隐私追溯

表1 牡蛎供应链全环节关键溯源数据

Tab.1 Key traceability data for oyster supply chain

所处环节	公开追溯数据	生物风险隐私数据
养殖环节	批次编号、批次数量、捕捞图像、捕捞时间、养殖资质、产地信息、养殖信息、生长周期	病原体名称、样品编号、生物风险因子类别、扩增子序列、典型序列、检测时间、检测地点、检测人、风险等级
加工环节	批次编号、包装批次编号、加工资质、加工企业、加工方式、加工日期	
仓储环节	批次编号、入库批次编号、仓储资质、仓储地点、温湿度、出入库时间	
物流环节	批次编号、物流批次编号、物流资质、运输时间、物流企业、运输路线、温湿度	
销售环节	批次编号、销售资质、销售来源、销售地、销售时间	

数据是由产品批次编号和产品检测编号分别进行查询。数据上链持久化存储后产生交易哈希值，该值是区块链中每一笔交易的唯一标识符。上链数据如表 2 所示。

表 2　上链键值对数据

Tab. 2　Key-value data of traceability blockchain

键	追溯数据值	交易哈希值	区块高度
20241001 − ZJHZ − BatchNum01	公开溯源数据	0xb093906f7978a3446f9468f5971d5eaecec11ecc4b2de1cc45d2aa6556fc43461	17 676
20241001 − ZJHZ − Detect01	检测报告密文哈希值	0xd03f63d15d4b9d21e4a08f129a0ae4e60dd871e5e05ff0f1a50076b69e18f40c	17 677

1.2　牡蛎供应链生物风险因子溯源区块链模型构建

目前，区块链技术在生物风险因子监管方面的研究较少。生物风险因子追溯系统是牡蛎在不同环节的样本进行抽样检测后数据上链存储，做到数据隐私保护和数据查询优化的平台。由于中心化的存储平台存在恶意篡改数据，数据不透明的问题，研发基于区块链的传带性生物风险因子溯源系统，用于实现生物风险数据的可信溯源。该系统能够在不同环节将样本抽样检测的数据安全上链、预警和追溯。本研究中将可搜索加密算法和构建密文倒排索引作为溯源模型的核心，为监管者高效地提供数据支撑。牡蛎供应链溯源区块链模型如图 1 所示。

在牡蛎供应链管理中，各企业将检测样品送至

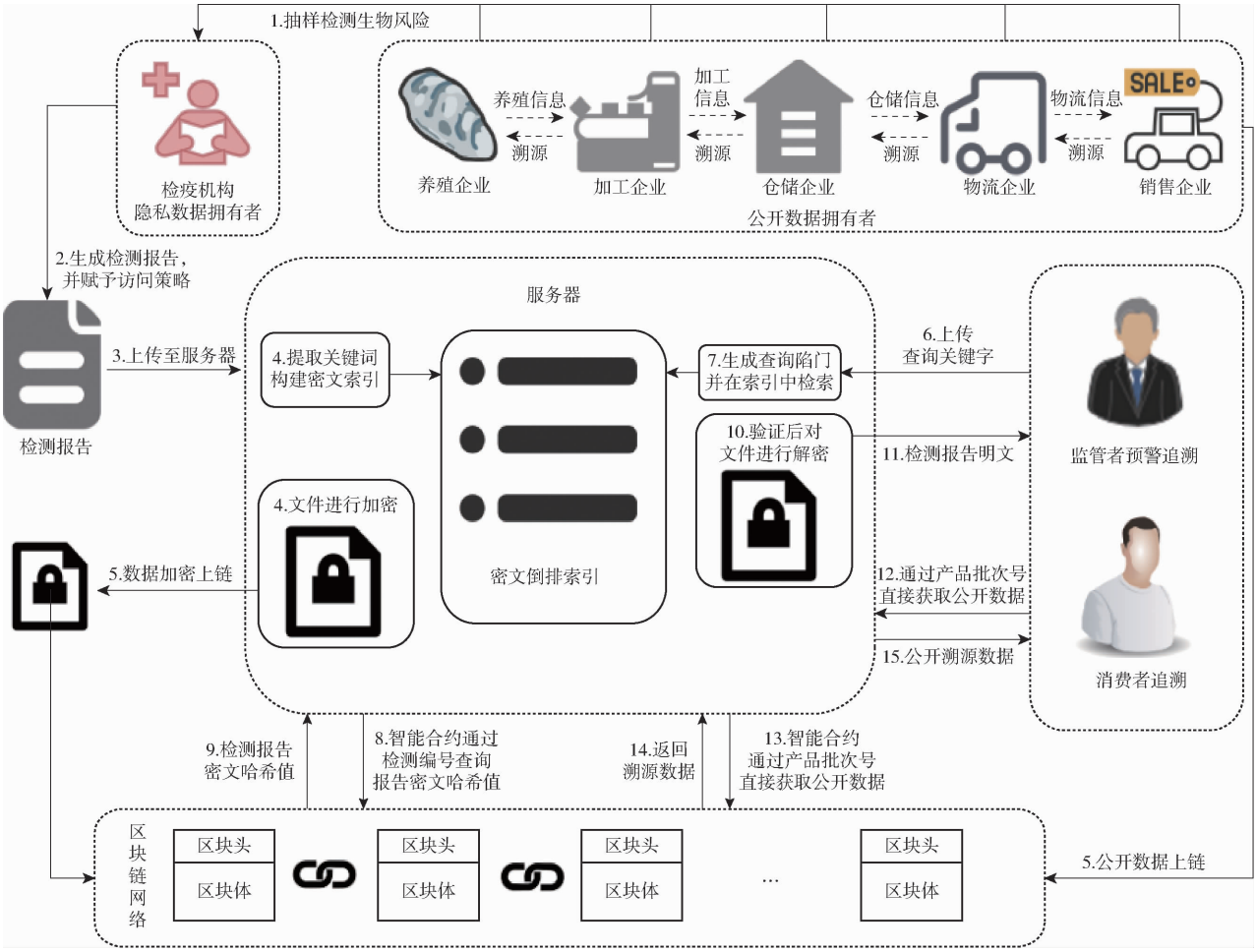

图 1　牡蛎供应链溯源区块链模型

Fig. 1　Oyster supply chain traceability blockchain model

检疫机构进行生物风险因子的抽样检测，检测完成后生成的报告会上传到系统中，并指定可以访问数据的角色。系统不仅提取检测报告中的关键信息，如生物风险因子的种类和检测样品的批次号，还对这些信息及完整的检测报告根据属性集合以及访问策略进行加密处理，以确保数据的安全性和隐私性。为了便于监管者进行高效查询，系统利用加密后的关键字和样品批次号构建了一个可搜索的加密倒排索引，并将所有完整的数据密文安全地存储在区块链上。

当监管者需要查询特定日期，以及包含特定生物风险因子如“大肠杆菌”的所有检测数据时，只需

在系统中输入相应的日期和关键词。系统将根据输入的关键词,基于监管者的属性私钥以及其公钥生成一个关键词的陷门,这个陷门能够与倒排索引中的加密关键字进行匹配计算,快速定位到包含该关键词的所有数据。系统随后筛选出与查询日期相匹配的检测样本编号,并通过智能合约自动执行查询该样本编号的密文哈希值,获取到相应的检测报告密文哈希值,并与数据库里检测文件的密文哈希值进行数据的验证,确保数据未被篡改。最后,系统将这些密文数据解密,展示给监管者,确保监管者能够及时获取所需的关键信息。

2 生物风险因子隐私数据的访问控制和查询优化

2.1 生物风险因子隐私数据共享模型

2.1.1 隐私数据共享模型

本文的数据共享模型如图 2 所示,共包含:属性授权中心(Authorization center, AC);数据属主(Data owner, DO),包括上传公开溯源数据的主体企业和上传生物风险隐私数据的检疫机构;数据用户(Data user, DU),包括消费者和监管者;服务器(Service provider, SP)。DO、DU、AC 和 SP 共同构成生物风险数据共享系统,支持对所有用户的公开溯源数据和生物风险隐私数据存储、管理、搜索、共享等服务。用户通过身份注册后可以使用该系统,自主定义数据共享规则(即访问控制策略)。

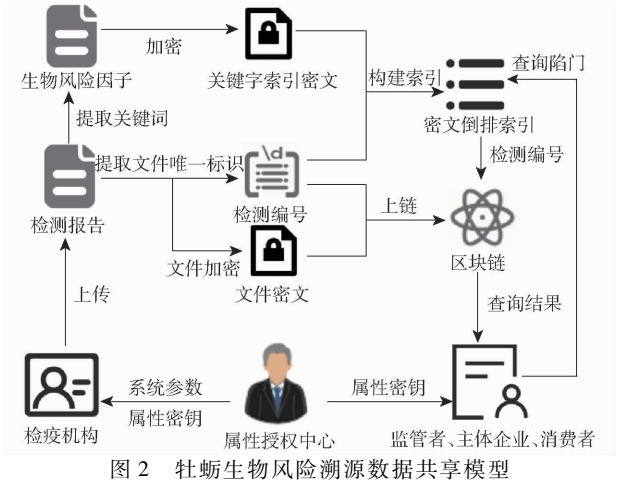

图 2 牡蛎生物风险溯源数据共享模型

Fig. 2 Oyster biological risk tracing data sharing model

对数据共享模型中的 5 个主体描述如下:

(1)属性授权中心:属性授权中心是以代码的形式集成在系统中,作为整体系统的一部分。它负责生成和管理系统的公共密钥和主密钥。公共密钥公开给所有用户,主密钥由属性授权中心管理,用于生成用户的私钥。属性授权中心根据用户的属性信息,使用主密钥生成用户的私钥,并通过安全信道分发给用户。例如,若系统中某用户的属性为“角色:牡蛎养殖基地”,则属性授权中心会为其生成包含对应属性解密密钥的私钥。这样,用户便能利用该私钥解密那些针对“牡蛎养殖基地”角色加密的数据,确保只有具备相应属性的用户能够访问特定的敏感信息,从而实现精准且安全的数据共享。

(2)数据属主:是指对牡蛎供应链中生物风险因子负责检测的检疫机构和供应链中的企业,检疫机构将要加密的检测文件 $F=\{F_1,F_2,\cdots,F_n\}$ 上传至系统,检疫机构在上传的过程中制定隐私数据可被访问的权限,然后根据访问策略加密生成的密文和同时生成检测文件的关键字索引 $I=\{I_1,I_2,\cdots,I_n\}$,并上传至区块链存储,当数据访问者满足访问策略时,访问者对关键字具有搜索权限和解密密文。

(3)数据用户:是指对生物风险因子的监管者、对应隐私数据的主体企业和消费者。当数据访问者需要查询包含关键字索引的生物风险隐私数据时,提交自身用属性授权中心分发的属性私钥、公共参数和关键字构造搜索令牌,生成搜索令牌提交至系统,获取到与关键字匹配的数据密文哈希值,将隐私数据密文哈希值与数据库中对应检测文件的密文哈希值进行验证,并利用私钥对检测文件的密文进行解密,若满足属性策略的要求,即可正确访问生物风险因子检测数据。

(4)服务器:服务器作为生物风险因子隐私数据共享与检索的服务提供方,主要负责数据的处理与存储。它执行隐私数据的加密与解密服务,处理上传时的隐私数据加密请求,确保数据在上链前被正确加密,同时也处理用户访问时的解密请求,利用由属性授权中心生成并分发给用户的私钥来解密数据。此外,服务器还提供倒排索引的生成和查询匹配处理。在牡蛎农产品供应链中,服务器为检疫机构提供了一个安全的上传接口,利用加密通信和身份验证机制,确保检测报告的安全上传,监管者可以查看所有数据,企业根据其属性获取或上传数据,而消费者仅能访问公开数据。属性管理、策略制定与执行以及密钥的生成与分发,则是由属性授权中心专门负责,服务器与之协作,共同维护系统的安全性和功能性。

(5)区块链网络:本文将牡蛎供应链中的隐私数据和公开数据上链存储,区块链的数据一旦记录几乎不可能被篡改,确保了隐私数据的真实性和可靠性。通过使用区块链技术,建立一个去中心化的数据共享平台,所有参与方如检疫机构、监

管者、农产品供应链企业及消费者可以在该平台上安全地交换和访问数据，解决了传统供应链数据只存在企业本地数据库所带来的数据孤岛问题。

2.1.2　隐私数据共享流程

检疫机构首先将待加密的检测报告、访问策略和自身属性信息提交至系统。系统随后从文件中提取关键字，生成加密文件索引和密文。然后，系统将文件的检测编号与密文文件索引数据一起添加到倒排索引列表中。同时，检测编号和密文被上传至区块链网络。在这一过程中，系统调用数据上链智能合约，将检测编号和文件密文以键值对（key - value）的形式存储在区块链中，实现数据的持久化。

当搜索者需要检索隐私数据时，需上传个人属性、搜索关键词及全网属性。系统据此生成一个搜索令牌，并用它与倒排索引中的密文索引进行匹配，以识别相关的词项。一旦找到匹配项，系统将在倒排列表中进一步筛选数据。成功检索后，搜索者将获得相应的检测批次编号，并将此编号上传至区块链。随后，系统调用监管智能合约，节点会将相应的密文哈希值发送给搜索者。最终，搜索者使用自己的属性信息对收到的密文哈希值进行验证及解密，以获取原始文件内容。隐私数据共享流程如图 3 所示。

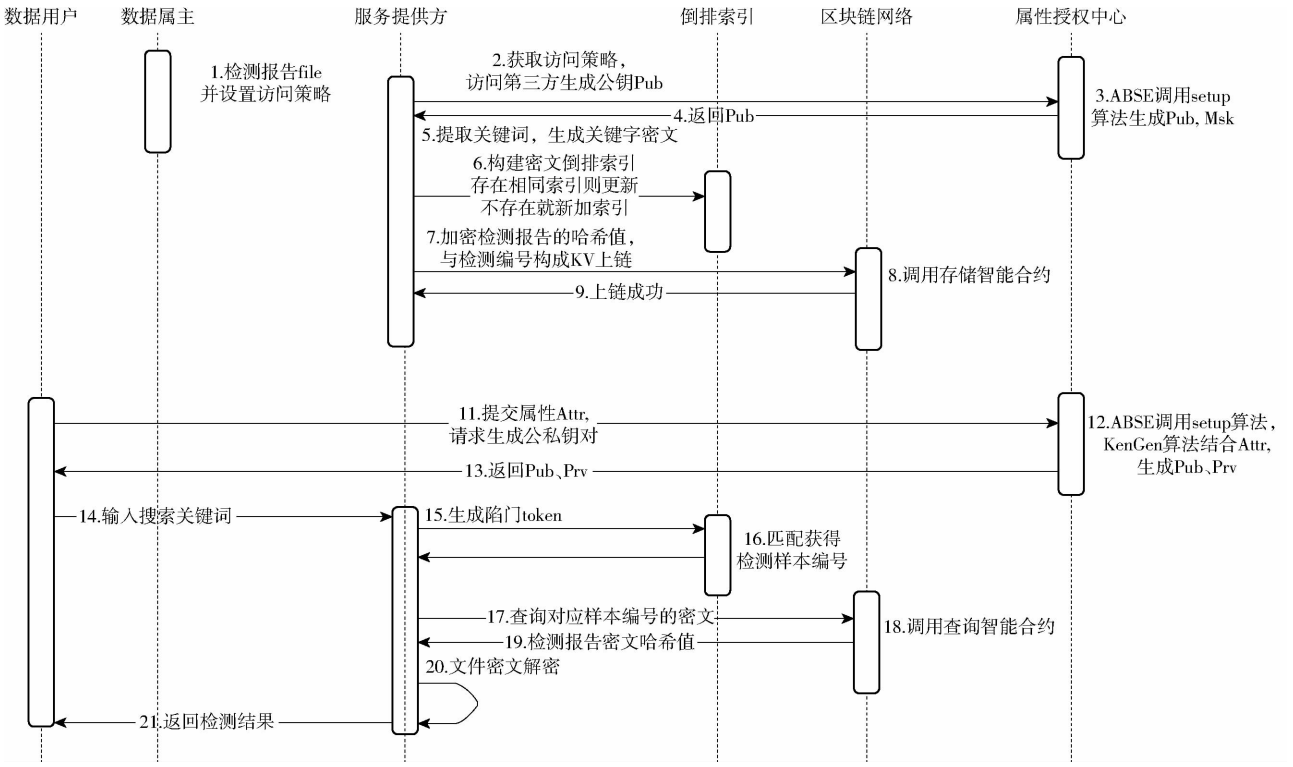

图 3　隐私数据共享流程

Fig. 3　Privacy data sharing process

2.2　基于属性的可搜索加密算法

基于属性的可搜索加密算法允许用户在加密数据上进行基于属性的搜索查询。这种技术结合了属性基访问控制和可搜索加密的优点，使得数据所有者能够对数据进行加密，同时授权特定用户或用户组基于特定属性检索信息。在生物风险因子监管的场景下，对牡蛎产品的生物风险检测文件应当只有对应的主体企业以及监管者有权限进行查看，其他企业和消费者无权查看。因此本文使用基于属性的可搜索加密算法使得检疫机构能够对检测报告赋予访问权限，指定可以访问该份文件的主体，保证数据安全的情况下增加访问的灵活性。

2.2.1　系统初始化

（1）设置全局属性 U

确定系统中将用于访问控制的属性集 $U = \{\mathrm{Attr}_1, \mathrm{Attr}_2, \cdots, \mathrm{Attr}_n\}$。在牡蛎供应链中，这些属性可能包括供应链角色（如检疫机构、监管者、养殖企业、加工企业、仓储企业、物流环企业、销售企业）、地理位置、产品类型等。

（2）算法初始化

$\mathrm{TSetup}(\lambda) \rightarrow (\mathrm{Pub}, \mathrm{Msk})$：初始化阶段算法选择群生成算法 PairGen 生成循环群组。当输入安全参数 λ 时，得到同为 p 阶的群组 (G_0, G_1)，构造对称的双线性映射函数 $e_0, e_0: G_0 \times G_0 \rightarrow G_1$。生成在椭圆曲线上的随机点 g_1、g_a、g_b、g_c 和 g_2，并在有限域 Z_r 生

成随机的主密钥元素 a、b 和 c，计算 $g_a = g_1^a$、$g_b = g_1^b$ 和 $g_c = g_1^c$，初始化公共参数数组，生成每个属性 Attr_i 对应的随机有限域元素 r_i 和随机群元素 x_i，计算 $y_i = e(g_1, x_i)$ 和 $u_i = g_1^{-r_i}$。最后生成公钥 Pub 和主密钥 Msk，公式为

$$\mathrm{Pub} \leftarrow (g, g_a, g_b, g_c, u_i, y_i) \tag{1}$$

$$\mathrm{Msk} \leftarrow (a, b, c, r_i, x_i) \tag{2}$$

2.2.2 用户注册

KeyGen(Msk, U)→Prv：系统通过属性授权中心给用户分发密钥，用户通过注册流程向属性授权中心提交其属性信息，属性授权中心根据用户的属性和访问控制策略生成一个私钥。该私钥由属性授权中心分发给用户，用户通过该私钥可以解密符合访问策略的密文。该阶段供应链中的各个企业包括检疫机构和监管者向属性授权中心申请各自的私钥。首先获取属性数组 U 的长度 len，初始化私钥对象 Prv(sig[ ], y[ ], v, sig_user, y_user) 的属性值，其中 sig[ ] 和 y[ ] 用于存储签名和配对结果，v、sig_user 和 y_user 是群元素，用于存储中间计算结果。计算 v 的值，即 $v = \mathrm{pub}.\ g_2^{Msk.a * Msk.c}$。对于每个属性 $u[i]$，如果企业属性 Attrs 包含 $u[i]$，则计算 sig[i]，公式为

$$\mathrm{sig}[i] = \mathrm{Prv}.\ v^{r[i]}\ \mathrm{Msk}.\ x[i] \tag{3}$$

否则计算 Prv. sig[i]，公式为

$$\mathrm{sig}[i] = \mathrm{Prv}.\ v^{r[i+\mathrm{len}]}\ \mathrm{Msk}.\ x[i+\mathrm{len}] \tag{4}$$

初始化 Prv. sig_user = Prv. sig[0] 和 Prv. y_user = Prv. y[0] 为第 1 个属性的签名和配对结果，对于剩余的属性，依次将签名和配对结果相乘，最终得到 Prv. sig_user、Prv. y_user 并返回 Prv，公式为

$$\mathrm{sig_user} = \prod_{i=1}^{\mathrm{len}-1} \mathrm{sig}[i] \tag{5}$$

$$\mathrm{y_user} = \prod_{i=1}^{\mathrm{len}-1} y[i] \tag{6}$$

2.2.3 检测数据关键词密文生成

Encrypt(U, Pub, policy, index)→cph：检疫机构在上传生物风险因子检测报告时，会指定一个访问策略 policy，这个策略定义了可以访问这些数据的用户。系统首先创建一个新的加密对象 cph，包括 w_0、w 和 u_gate。接着计算了两个基于索引 index 的固定值 t_1 = hash(index. word) 和 t_2 = hash(index. word)，并通过哈希函数将索引词 index. word 映射到群的标量域中，得到待加密的元素 m。并将它们用于计算中间变量 $w_{01} = (\mathrm{Pub}.\ g_a)^{\mathrm{add}}$，其中 add = $t_1 + t_2$、$w_{02} = (\mathrm{Pub}.\ g_a)^{t_1}$，最后得到密文组件

$$w_0 = (\mathrm{Pub}.\ g_c)^{t_1} \tag{7}$$

$$w = w_{01}(w_{02})^m \tag{8}$$

$$u_gate = (\mathrm{Pub}.\ g_1)^{t_2} \tag{9}$$

然后，根据检疫机构上传的访问策略，遍历用户属性数组 Attr 和策略数组 policy。如果用户属性满足访问策略的要求，系统会更新加密过程中使用的 u_gate 值，它的值会根据用户的属性进行调整，以确保只有满足策略的用户才能正确解密数据。最终，返回包含加密结果的密文，该密文只能在满足特定访问策略的授权用户处解密。

2.2.4 原始检测文件加密

检疫机构上传原始检测文件后，系统生成一个随机长度为 32 位的 AES 密钥 K。定义初始化向量 IV，使用 AES－CBC(Advanced encryption standard－cipher block chaining) 模式加密检测文件 file，得到密文 C，$C = E_{\mathrm{AES-CBC}}(K, \mathrm{IV}, \mathrm{file})$。随后对 AES 密钥 K 进行属性基加密保护，根据策略 policy 生成加密后的 AES 密钥 K'，$K' = E_{\mathrm{ABE}}(\mathrm{policy}, K)$。对加密后的 AES 密钥 K' 和密文 C 进行 Base64 编码，获得 $K'' = \mathrm{Base64}(K')$，$C' = \mathrm{Base64}(C)$。最后将编码后的 AES 密钥 K'' 和加密后的文件内容 C' 写入到新的文件中，根据文件提取的关键词经过特殊编码作为文件的唯一标识符。在文件持久化之前，使用 SHA－256 哈希算法为每个文件生成唯一的哈希值，用于后续的数据验证。最后将文件哈希值与文件标识符上链存储。

2.2.5 关键词密文匹配

(1)搜索令牌生成

Trapdoor(Pub, Prv, word)→token：生成搜索令牌算法，用于监管者和隐私数据对应主体企业在加密数据中搜索特定的关键字。生成的陷门包含了用户属性的信息，确保只有拥有正确属性组合的用户才能生成有效的陷门并成功执行查询。算法初始化了一个新的对象 token。包含 5 个 Element 类型的对象 tok1 ~ tok5，这些对象用于存储生成令牌过程中需要的各种元素。创建了一个随机数 s 作为生成令牌的一部分私钥，同时创建了对象 wm 来存储要加密的关键字的哈希值，wm = wm. setFromHash(w, 0, w. len) 将字符串转换成一个有限域上的元素。随后，计算 tok1 ~ tok5，其中 tok1 = $((\mathrm{Pub}.\ g_b)^{\mathrm{wm}}\mathrm{Pub}.\ g_a)^s$，tok2 = $(\mathrm{Pub}.\ g_c)^s$，tok3 = $(\mathrm{Prv}.\ v)^s$，tok4 = $(\mathrm{Prv}.\ \mathrm{sig_user})^s$，tok5 = $(\mathrm{Prv}.\ \mathrm{y_user})^s$。最终，方法返回生成的 token 对象。

(2)关键字匹配

Search(Pub, token, cph)→res：关键字匹配算法使用用户提供的 token 与生物风险因子隐私数据进行匹配。算法初始化一个布尔变量 res 来存储

搜索结果，然后使用双线性配对 pairing 来计算中间值，即

$$E = \frac{e(\text{u_gate}, \text{tok3})\, e(g_1, \text{tok4})}{\text{tok5}} \tag{10}$$

然后，创建两个新的元素 left 和 right，并分别计算，即

$$\text{left} = e(w_0, \text{tok1})\, E \tag{11}$$

$$\text{right} = e(w, \text{tok2}) \tag{12}$$

最后，代码比较 left 和 right 是否相等，如果相等，则将 res 设置为 true，表示搜索条件满足。该方法最终返回结果 res，表示搜索操作的结果。

2.2.6　原始检测数据解密

监管者提交所要查询的关键字以及对应牡蛎农产品货物的日期范围，在密文倒排索引中进行数据的检索，获取到文件的唯一标识符后，使用区块链智能合约通过文件唯一标识符查询到文件哈希值。将区块链上查询到的文件哈希值与数据库里的文件的哈希进行对比，确保数据未被篡改。随后读取加密文件 file，读取其加密的 AES 密钥 K'以及加密的文件内容 C'。对加密的 AES 密钥 K'和加密的文件内容 C'进行 Base64 解码，得到原始的字节序列，$K'' = \text{Base64Decode}(K')$，$C = \text{Base64Decode}(C')$。之后系统使用属性基解密对加密的 AES 密钥 K''进行解密，根据用户的属性 Attrs 恢复出原始的 AES 密钥 K。$K = D_{\text{ABE}}(\text{Attrs}, K'')$。最后使用恢复出来的 AES 密钥 K 对加密的文件内容 C 进行解密，得到原始文件内容 $\text{file} = D_{\text{AES-CBC}}(K, \text{IV}, C)$。

2.3　倒排索引对关键字密文数据的查询优化

倒排索引的核心思想是将文档中出现的单词映射到包含这些单词的文档列表，从而实现快速检索。在倒排索引中，所有单词被称为“词项字典”，每个单词对应一个倒排列表，其中包含多个文档的引用。这些引用通常包括文档 ID 和词条在文档中的位置信息。当用户提交查询时，服务器会查找与查询条件匹配的词条，然后迅速定位到包含这些词条的所有相关文档唯一索引。

为了提高生物风险因子密文数据的查询效率，引入了倒排索引技术。构建牡蛎检测文件的密文倒排索引，快速查询出所有包含相关词项的数据，能够大幅提高检测报告数据检索效率。然而，由于需要对每个文档进行分词处理并建立倒排列表，当文档量很大时，处理时间较长。其次，倒排索引需要维护大量的词项列表和倒排列表，增加了存储和管理成本。在生物风险因子监管的场景下，为了避免大量无效的词项去构建索引，并且对无效的词项进行加密也是极大的资源浪费，因此文本优化了分词方案，只提取生物风险因子种类的数据去构建密文索引，减少无效的词项。同时针对倒排列表中的检测编号明文存储，并进行特殊编码设计，例如：20241001 - Detect001 - ZJHZ，在不泄露任何有效信息的同时，也方便监管者对数据的检索，减少密文数据的匹配计算，提高查询效率。

在本文中，检测机构将生物风险检测报告填写并提交至追溯系统。系统首先对每个数据项中的文本内容分词，将其转换为单独的关键字。然后使用基于属性的可搜索加密算法生成加密的关键字，并将其与数据的检测编号以 key - value 集合的形式构建出文件索引。当索引中没有相同的关键字密文索引时，会生成新的索引添加到倒排索引中，反之直接将 value 添加到对应关键字的倒排列表中。

监管者可以通过密文搜索索引对生物风险因子数据进行查询。该索引结构如图 4 所示，包括 3 个主要部分：词项字典、倒排列表和文档频率。词条字典包含所有加密关键词。而倒排列表则针对每个加密的关键字创建一个索引列表，该列表包含指向包含该词条的所有加密数据的指针。在本系统中，这些指针是数据对象唯一检测编号。文档频率表示该关键字在文档集合中出现的文档数量，用于辅助监管者判断该关键字在供应链中的重要性。

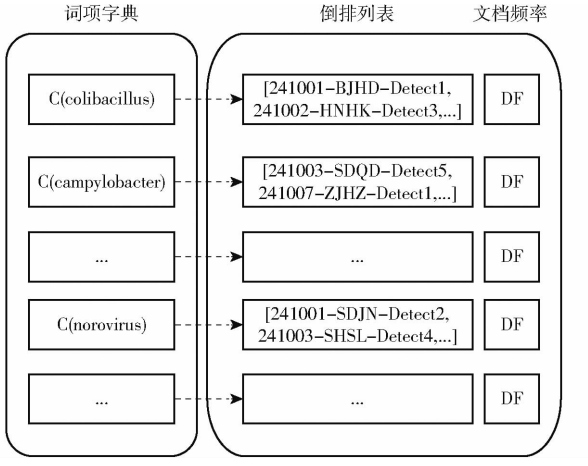

图 4　索引结构

Fig. 4　Index structure

当监管者进行检索时，假设其检索词为“大肠杆菌”“20241010”，上传至系统会根据监管者的公私密钥和关键词生成搜索 Token，系统将在词项字典中进行关键字密文的匹配，从而快速查询到所有包含“大肠杆菌”的牡蛎货物的检测编号，经过时间的筛选得到精确的检测文件编号，根据检测文件编号在区块链中查询出对应的数据密文哈希值，并使用其私钥对数据密文进行解密以访问原始数据。以牡蛎养殖环节的检测报告为例，具体算法如下：

算法 1:索引的添加与更新
输入:生物风险因子种类的密文值、对应的检测编号
输出:存在同样的关键词则更新索引,不存在则添加索引返回

```
1. Function 〈insert〉([〈key:cph〉,〈detectNumber:String〉])
2. Begin
3. fid:FreqAndId
4. fId←dir.get(key)
5. if 〈fId == null〉 Then
6.    Begin
7.    fId←new FreqAndId()
8.    fId.addFreq()
9.    dir.put(key, fId) //添加成功
10.   End
11. Else
12.   Begin
13.   if (! fId.postingList.contains(detectNumber))
14.      Begin
15.      fId.addFreq()
16.      fId.adddocId(detectNumber) //更新成功
17.      End
18.   End
19. End insert
```

算法 2:数据在倒排索引中的查询
输入:查询陷门,具体日期
输出:样本检测批次号

```
1. Function〈search〉([〈pub:Pub〉,〈token:Token〉,〈time:String〉])
2. Begin
3. list←new ArrayList〈〉()
4. for (Map.Entry〈Object,FreqAndId〉 entry : dir.entrySet())
5.    Begin
6.    Object c = entry.getKey()
7.    res = Bswabe.search(pub, token, cph) //匹配过程
8.    If (res == true)
9.       Begin
10.      freqAndId←entry.getValue()
11.      arrayList←(ArrayList〈String〉) freqAndId.postingList //获取到数据
12.      Index←binarySearch(arrayList,time) //二分查找筛选数据
13.      break
14.   End
15.   End
16. return arrayList.get(index)
17. End search
```

2.4 智能合约设计

通过与以太坊平台的结合,确保了数据的分布式存储、去中心化特性以及不可篡改性。系统的数据模型设计考虑了生物风险数据的结构、属性和实体间关系,定义了病原体、疾病、病例、检测结果等关键实体。数据查询,数据预警智能合约使用 solidity 语言编写,规范了数据的创建、修改和查询流程,并结合牡蛎供应链实际情况等制定相关的智能合约规则和一系列合约触发条件。智能合约业务逻辑设计如表 3 所示。

表 3 智能合约设计

Tab.3 Smart contract design

合约功能	合约方法	输入	输出	描述
数据上链合约	recordAquaculture()	养殖环节数据	True/False	公开溯源数据及其牡蛎农产品批次号上链存储
	recordProcess()	加工环节数据	True/False	
	recordTransport()	运输环节数据	True/False	
	recordWareHouse()	仓储环节数据	True/False	生物风险隐私数据密文哈希值及其检测编号上链存储
	recordSale()	销售环节数据	True/False	
	recordSupervision()	生物风险因子密文检测数据	True/False	
公开数据查询合约	queryRecore()	牡蛎批次号	牡蛎批次信息	链上公开溯源数据查询
隐私数据监管合约	querySupervision()	样本检测批次号	生物风险因子密文哈希值	生物风险隐私数据密文哈希值查询

将牡蛎供应链各个环节的溯源信息写入区块链和查询数据均由智能合约实现。以养殖环节的隐私数据查询方法为例,具体算法如下:
算法 3:隐私数据查询智能合约算法
输入:检测样本编号
输出:对应批次的密文哈希值

```
1. Function〈querySupervision〉(〈id:DetectNumber〉)
2.    Begin
3.       require(id > 0, "Invalid ID") //检查 id 是否为有效值
4.       Data storage data ← dataMap[id] // 检查 dataMap 中是否存在给定的 id
```

```
5.        if (data.id == = 0) //确保数据存在
6.        Begin
7.        emit DataNotFound(id)
8.        revert("Data not found")
9.        End
10.       require (bytes (data. cph). length > 0,
"Incomplete data")
11.       emit DataRetrieved(id, data.cph) //记录日
志
12.       return data.cph //返回 cph 哈希值
13.   End querySupervision
```

3　实验测试与系统实现

3.1　实验测试分析

本实验在主机配置为 3.2 GHz、AMD Ryzen7 - 5800h CPU、16 GB RAM，系统为 Windows 11 下进行测试，在本节中，测试了该方法的密文搜索和陷门生成时间，并对可搜索密文与陷门的匹配时间进行了性能测试。由于本文的用户属性主要包括监管机构、检疫组织以及供应链各环节的主体企业。基于此对不同属性数量的访问控制开销进行实验。为了保证数据的客观性，对每组数据各执行 10 次，求平均值并记录。实验结果表明，基于属性的可搜索加密算法关键字密文生成时间平均为 31 ms，陷门生成时间平均为 32 ms，匹配计算时间平均为 16 ms，对于检测文件进行加密平均时间为 141 ms，检测文件解密时间平均为 26 ms，实验结果如图 5 所示。

此外，还测试了密文搜索效率，并将这些性能指标与文献[25]中提出的新型倒排索引可搜索加密方案以及文献[30]的基于属性可搜索加密的访问控制方法进行了对比分析。文献[25]的新型倒排索引通过密文形式存储关键字和文档信息，并使用伪随机函数生成速查表 Ts 的节点信息，确保恶意服务器在无密钥情况下无法区分不同关键字的输出；随着文档数量增加，密文搜索开销逐渐增大。本文中的倒排索引针对提取的生物风险因子关键词进行加密，同时采用特殊编码的检测编号明文存储在倒排列表中，减少了大量数据加密带来的计算和存储开销，在保证数据安全的同时提高了检索效率。实验表明，本文的数据检索开销增长速率更为缓慢，更加符合实际应用场景；在每个关键字对应 100 个文档的情况下，平均检索时间为 385 ms，如图 6a 所示。文献[30]解决了访问策略泄露敏感信息的问题，其查询匹配时间为 3.54 ms，性能较高，但需要对密文列表中的所有密文逐个查询匹配，导致查询时间与密文数量呈正比关系。本文在

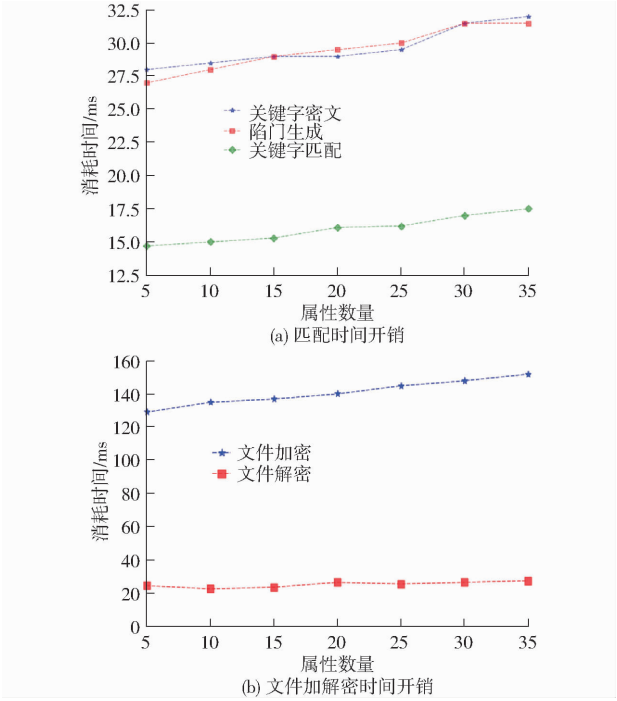

图 5　基于属性可搜索加密算法的时间开销

Fig. 5　Cost of attribute-based searchable encryption algorithms

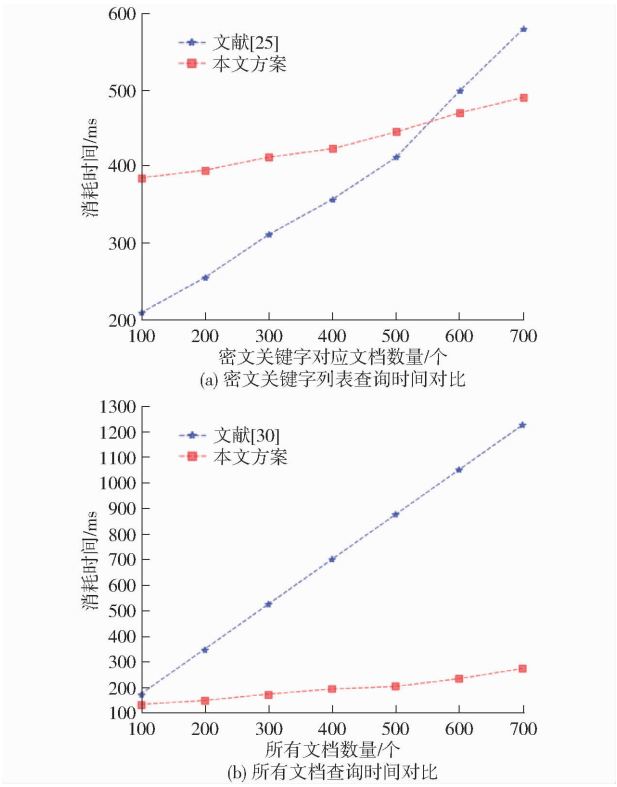

图 6　数据检索时间开销

Fig. 6　Cost of data retrieval

默认索引结构下，词项列表对应的倒排列表数据个数为 10 时，与未添加索引结构的文献[30]相比，查询时间显著减少，结果见图 6b。

3.2　系统设计与实现

牡蛎供应链生物风险因子溯源系统架构如

图 7 所示,共分为 4 层:应用层、接口层、服务层和区块链层。应用层包括政府部门监管、消费者溯源和生物风险数据采集,分别用于监管、产品追踪和生物风险数据管理。接口层提供 RPC 接口、数据查询接口、访问控制接口和数据上传接口,用于不同服务间的通信、数据查询、访问管理和数据上传。服务层包含企业注册、数据加密/解密、数据匹配和数据检索,涉及企业属性验证、数据安全、密文数据匹配和检索功能。区块链层由智能合约、分布式存储、共识算法和默克尔交易树组成,实现自动执行合约、数据安全存储、网络一致性和交易数据的高效验证。



图 7 系统架构图

Fig. 7 System architecture

在实验中,通过与检疫机构的深入交流,详细了解了其在检测信息管理方面的需求和相关数据,并设计了系统的各个功能模块。以 2024 年 10 月 3 日为例,模拟了一个场景,假设其中在检疫机构检测出牡蛎农产品含有大肠杆菌的生物风险因子。如图 8、9 所示,检疫机构的工作人员登录到生物风险溯源系统,并将详尽的检测信息录入系统并指定对应的该检测信息可被访问的属性角色,实现数据的访问控制。



图 8 系统主界面

Fig. 8 System main interface



图 9 检测报告上传

Fig. 9 Test report upload

当系统接收到检疫人员发送的数据请求时,自动提取生物风险因子的关键信息,并对该信息及其检测文件进行加密处理。随后,系统会创建生物风险因子的密文关键词索引,并将该密文索引与唯一标识符检测编号一同构建倒排索引,如果系统未曾将该密文关键词索引添加至倒排索引中,系统将自动创建一个新的索引条目,如图 10 所示。反之,更新对应密文关键词索引的词项列表。



图 10 添加索引

Fig. 10 Add index

系统通过将检测报告的密文哈希值及检测批次信息记录在区块链上,利用智能合约构建交易,将关键数据安全地添加至区块链中,如图 11 所示。监管人员仅需输入特定的生物风险因子和查询日期,系统便能迅速通过索引定位相关检测编号。随后,系统通过智能合约在区块链上执行精确搜索,获取检测报告的密文哈希值。最后将加密的检测报告解密,展示给监管人员,如图 12 所示。最后系统将加密的检测数据解密,返回给前端进行解析展示给监管人员查询数据结果,如图 13 所示。



图 11 数据上链成功

Fig. 11 Data on blockchain successfully



图 12　链上数据查询

Fig. 12　Data query on blockchain



图 13　追溯数据展示

Fig. 13　Retrospective data presentation

4　结束语

本文研究了在保证牡蛎供应链中生物风险因子检测数据隐私安全的同时，对于监管者和主体企业依然能够对隐私数据进行数据的检索。本文针对牡蛎供应链建立区块链网络，各主体企业上传公开追溯数据，检疫机构上传供应链中各环节对牡蛎农产品的生物风险因子检测数据，并结合基于属性的可搜索加密算法和倒排索引技术，实现了生物风险因子隐私数据的访问控制和高效查询。最后，开发了生物风险因子溯源原型系统，相关测试结果表明了可搜索加密算法和倒排索引技术的方法性能，验证了方法的可行性，在关键字为密文的情况下，每个关键字对应文档为 100 个的情况下，检索时间平均为 385 ms，系统性能满足牡蛎供应链风险因子监管溯源的需求，为解决农产品食品安全问题提供了参考。

参　考　文　献

[1] 邹一波，李清雨，陈明，等. 基于生食牡蛎 HACCP 计划的语义建模研究[J]. 农业机械学报，2021，52(12)：290－299.
ZOU Yibo, LI Qingyu, CHEN Ming, et al. Semantic modeling based on raw oyster HACCP program[J]. Transactions of the Chinese Society for Agricultural Machinery, 2021, 52(12): 290－299. (in Chinese)

[2] LOVE D C, LANE R M, KUEHL L M, et al. Performance and conduct of supply chains for United States farmed oysters[J]. Aquaculture, 2020, 515: 734569.

[3] SCHROBBACK P, ROLFE J, RUST S, et al. Challenges and opportunities of aquaculture supply chains: case study of oysters in Australia[J]. Ocean & Coastal Management, 2021, 215: 105966.

[4] 李漫，王卓琳，刘泽鹏，等. 生食牡蛎从离水到餐桌的安全与质量管理现状与对策[J]. 水产学报，2024，48(7)：18－25.
LI Man, WANG Zhuolin, LIU Zepeng, et al. Current situation and countermeasures for quality and safety management of raw oysters from out of water to table[J]. Journal of Fisheries of China, 2024, 48(7): 18－25. (in Chinese)

[5] GAO P, MOHD NOOR N Q I, MD SHAARANI S. Current status of food safety hazards and health risks connected with aquatic food products from Southeast Asian region[J]. Critical Reviews in Food Science and Nutrition, 2022, 62(13): 3471－3489.

[6] POUILLOT R, SMITH M, VAN DOREN J M, et al. Risk assessment of norovirus illness from consumption of raw oysters in the United States and in Canada[J]. Risk Analysis, 2022, 42(2): 344－369.

[7] 徐佳乐，赵璐，贾添慧，等. 2019—2023 年上海市临港地区市售牡蛎中人源诺如病毒污染的调查研究[J]. 食品安全质量检测学报，2024，15(20)：28－34.
XU Jiale, ZHAO Lu, JIA Tianhui, et al. Investigation of human norovirus contamination in commercially sold oysters from the Lingang Area of Shanghai from 2019 to 2023[J]. Journal of Food Safety and Quality, 2024, 15(20): 28－34. (in Chinese)

[8] IITEMBU J A, FITZGERALD D, ALTINTZOGLOU T, et al. Comparative description and analysis of oyster aquaculture in selected atlantic regions: production, market dynamics, and consumption patterns[J]. Fishes, 2023, 8(12): 584.

[9] WANG O, SOMOGYI S, CHARLEBOIS S. Mapping the value chain of imported shellfish in China[J]. Marine Policy, 2019, 99: 69－75.

[10] FENG H, WANG X, DUAN Y, et al. Applying blockchain technology to improve agri-food traceability: a review of development methods, benefits and challenges[J]. Journal of Cleaner Production, 2020, 260: 121031.

[11] HAN J W, ZUO M, ZHU W Y, et al. A comprehensive review of cold chain logistics for fresh agricultural products: current status, challenges, and future trends[J]. Trends in Food Science & Technology, 2021, 109: 536－551.

[12] SHAMSUZZOHA A, MARTTILA J, HELO P. Blockchain-enabled traceability system for the sustainable seafood industry[J]. Technology Analysis & Strategic Management, 2024, 36(11): 3891－3905.

[13] YELE S, LITORIYA R. Blockchain-based secure dining: enhancing safety, transparency, and traceability in food consumption environment[J]. Blockchain: Research and Applications, 2024, 5(2): 100187.

[14] SHAVERDIAN P. Start with trust: utilizing blockchain to resolve the third-party data breach problem[J]. UCLA Law Review, 2019, 66: 1242.

[15] 王利朋,关志,李青山,等. 区块链数据安全服务综述[J]. 软件学报,2023,34(1):1 - 32.
WANG Lipeng, GUAN Zhi, LI Qingshan, et al. Survey on blockchain-based security services[J]. Journal of Software,2023, 34(1):1 - 32. (in Chinese)

[16] WANG S, LUO N, XING B, et al. Blockchain-based proxy re-encryption access control method for biological risk privacy protection of agricultural products[J]. Scientific Reports, 2024, 14(1): 20048.

[17] 于合龙,陈邦越,徐大明,等. 基于区块链的水稻供应链溯源信息保护模型研究[J]. 农业机械学报,2020,51(8):328 - 335.
YU Helong, CHEN Bangyue, XU Daming, et al. Modeling of rice supply chain traceability information protection based on block chain[J]. Transactions of the Chinese Society for Agricultural Machinery,2020,51(8):328 - 335. (in Chinese)

[18] 李修华,罗潜,杨信廷,等. 面向小麦区块链追溯系统的分级监管模型设计与实现[J]. 农业机械学报,2023,54(3):363 - 371.
LI Xiuhua, LUO Qian, YANG Xinting, et al. Design and implementation of blockchain hierarchical supervision model for wheat supply chain[J]. Transactions of the Chinese Society for Agricultural Machinery,2023,54(3):363 - 371. (in Chinese)

[19] 张德俊,饶元. 农产品区块链多监管差分隐私共享模型设计[J]. 江苏农业学报,2024,40(4):740 - 752.
ZHANG Dejun, RAO Yuan, et al. Design of multi-regulation differential privacy sharing model for agricultural product blockchain[J]. Jiangsu Journal of Agricultural Sciences,2024,40(4):740 - 752. (in Chinese)

[20] 黄一才,李森森,郁滨. 云环境下对称可搜索加密研究综述[J]. 电子与信息学报,2023,45(3):1134 - 1146.
HUANG Yicai, LI Sensen, YU Bin. A survey of symmetric searchable encryption in cloud environment[J]. Journal of Electronics & Information Technology,2023,45(3):1134 - 1146. (in Chinese)

[21] ANDOLA N, GAHLOT R, YADAV V K, et al. Searchable encryption on the cloud: a survey[J]. The Journal of Supercomputing, 2022, 78(7): 9952 - 9984.

[22] SONG D X, WAGNER D, PERRIG A. Practical techniques for searches on encrypted data[C]// Proceeding 2000 IEEE Symposium on Security and Privacy. S&P 2000. IEEE, 2000: 44 - 55.

[23] BONEH D, DI CRESCENZO G, OSTROVSKY R, et al. Public key encryption with keyword search[C]// Advances in Cryptology-EUROCRYPT 2004: International Conference on the Theory and Applications of Cryptographic Techniques. Interlaken: Springer Berlin Heidelberg, 2004: 506 - 522.

[24] 冯涛,陈李秋,方君丽,等. 基于本地化差分隐私和属性基可搜索加密的区块链数据共享方案[J]. 通信学报,2023, 44(5):224 - 233.
FENG Tao, CHEN Liqiu, FANG Junli, et al. Blockchain data sharing scheme based on localized difference privacy and attribute-based searchable encryption[J]. Journal on Communications,2023,44(5):224 - 233. (in Chinese)

[25] 刘炜,白晓丹,佘维,等. 基于倒排索引的可搜索加密数据共享方案[J]. 计算机工程与应用,2023,59(10):270 - 279.
LIU Wei, BAI Xiaodan, SHE Wei, et al. Searchable encrypted data sharing scheme based on inverted index[J]. Computer Engineering and Applications,2023,59(10):270 - 279. (in Chinese)

[26] 陈宁江,刘灿,黄汝维,等. 云环境中抵御内部关键字猜测攻击的快速公钥可搜索加密方案[J]. 电子与信息学报,2021, 43(2):467 - 474.
CHEN Ningjiang, LIU Can, HUANG Ruwei, et al. Fast public key searchable encryption scheme against internal keyword guessing attack in cloud environment[J]. Journal of Electronics & Information Technology, 2021, 43(2): 467 - 474. (in Chinese)

[27] 孙传恒,杨晓虎,罗娜,等. 基于区块链的三文鱼冷链多链协同监管模型研究[J]. 农业机械学报,2024,55(1):360 - 370.
SUN Chuanheng, YANG Xiaohu, LUO Na, et al. Blockchain based salmon cold chain multi-chain collaborative supervision model[J]. Transactions of the Chinese Society for Agricultural Machinery,2024,55(1):360 - 370. (in Chinese)

[28] 李明福,王振华,许瑾,等. 植检实验室生物安全风险因子分级研究[J]. 质量安全与检验检测,2023,33(3):44 - 47.
LI Mingfu, WANG Zhenhua, XU Jin, et al. Study of the classification of plant phytosanitary laboratory for biosafety risk[J]. Quality Safety Inspection and Testing,2023,33(3):44 - 47. (in Chinese)

[29] 孙传恒,于华竟,罗娜,等. 基于智能合约的果蔬区块链溯源数据存储方法研究[J]. 农业机械学报,2022,53(8):361 - 370.
SUN Chuanheng, YU Huajing, LUO Na, et al. Blockchain traceability data storage method of fruit and vegetable foods supply chain based on smart contract[J]. Transactions of the Chinese Society for Agricultural Machinery,2022,53(8):361 - 370. (in Chinese)

[30] 刘晓辉,罗娜,邢斌,等. 基于属性可搜索加密的农产品区块链追溯隐私数据访问控制方法[J]. 农业机械学报,2024, 55(10):433 - 443.
LIU Xiaohui, LUO Na, XING Bin, et al. Attribute-based searchable encrypted agricultural blockchain traceability private data access control method[J]. Transactions of the Chinese Society for Agricultural Machinery, 2024, 55(10): 433 - 443. (in Chinese)

[31] 王少华,孙传恒,罗娜,等. 面向预制食品溯源的隐私数据加密共享方法研究[J]. 农业机械学报,2024,55(5):405 - 418.
WANG Shaohua, SUN Chuanheng, LUO Na, et al. Privacy data encryption sharing method for prepared food traceability[J]. Transactions of the Chinese Society for Agricultural Machinery,2024,55(5):405 - 418. (in Chinese)