doi:10.6041/j.issn.1000-1298.2026.19.039

水产品质量安全风险溯源系统访问控制模型研究

葛　艳[1,2]　赵浩栋[1]　张　枫[3]　邹一波[1,2]　王文娟[1,2]　陈　明[1,2]

（1. 上海海洋大学信息学院，上海 201306；2. 农业农村部渔业信息重点实验室，上海 201306；
3. 光明食品集团上海崇明农场有限公司，上海 200085）

摘要：鉴于危害分析与关键控制点（HACCP）质量溯源系统覆盖了企业的敏感数据，为保护企业的隐私数据，并兼顾企业因适应外部市场的不确定性而进行的动态调整，本文以巴氏杀菌蟹肉 HACCP 计划为例，结合 Fabric 多通道技术和基于属性的访问控制（Attribute based access control，ABAC）模型，提出了 HACCP 溯源系统的访问控制模型（HACCP traceability system access control model，HTSACM）。该模型根据巴氏杀菌蟹肉的 HACCP 计划国家标准提取溯源数据，给出数据的风险等级定义，并按照用户类别做出了访问需求定义。从不同用户的数据访问权限出发，构建数据的双通道结构，采用私有数据集合存储隐私数据，实现了敏感数据的独立存储。设计属性混合存储形式和策略灵活更新机制，增强了基于区块链访问控制的动态性，在此基础上构建基于区块链的访问控制模型。最终实现了基于双通道的 HACCP 溯源系统访问控制模型，此访问控制模型实现了对链上数据的细粒度访问控制。在保障关键数据透明化与可追溯性的基础上，企业敏感信息通过私有通道进行隔离存储与独立管理，有效避免外部溯源操作对其造成的影响，从而提升企业隐私数据的安全性与可控性。同时，模型能够适应企业发展过程中出现的组织结构变化、业务扩展等不确定性因素，具备良好的灵活性与可扩展性。实验结果表明，系统在引入安全访问控制模型后，仍可实现 300 笔/s 的吞吐量，在提升安全性与隐私保护能力的同时，并未对系统性能产生明显影响。

关键词：区块链；HACCP 溯源访问控制模型；双通道；私有数据集合

中图分类号：TS207.7；TP309　　**文献标识码**：A　　**文章编号**：1000-1298(2026)19-0414-13　　**OSID**：

Access Control Model of Aquatic Product HACCP Traceability System

Ge Yan[1,2]　Zhao Haodong[1]　Zhang Feng[3]　Zou Yibo[1,2]　Wang Wenjuan[1,2]　Chen Ming[1,2]

(1. *College of Information Technology*, *Shanghai Ocean University*, *Shanghai* 201306, *China*
2. *Key Laboratory of Fisheries Information*, *Ministry of Agriculture and Rural Affairs*, *Shanghai* 201306, *China*
3. *Guangming Food Group Shanghai Chongming Farm Co.*, *Ltd.*, *Shanghai* 200085, *China*)

Abstract: In view of the fact that the HACCP quality traceability system covers the sensitive data of enterprises, in order to protect the private data of enterprises and take into account the dynamic adjustment of enterprises to adapt to the uncertainty of the external market, taking the pasteurized crab meat HACCP plan as an example, combined the Fabric multi-channel technology and the attribute based access control (ABAC) model, the HACCP traceability system access control model (HTSACM) was proposed. This model extracted the traceability data according to the HACCP plan national standard of pasteurized crab meat, gave the definition of the risk level of the data, and defined the access requirements according to the user category. Starting from the data access rights of different users, a dual channel structure of data was constructed, and private data collections were used to store private data, realizing independent storage of sensitive data. The attribute hybrid storage form and flexible policy update mechanism were designed to enhance the dynamics of blockchain based access control, and on this basis, a blockchain based access control model was built. Finally, the HACCP traceability system access control model based on dual channels was implemented, and this access control model implemented the fine-grained access control of data on the chain. On the basis of ensuring the transparency and traceability of key data, enterprise sensitive information was isolated, stored and

收稿日期：2025-06-27　修回日期：2025-07-24

基金项目：广东省重点领域研发计划项目(2021B0202070001)

作者简介：葛艳(1974—)，女，副教授，博士，主要从事质量安全风险评价、溯源和农业信息化研究，E-mail：yge@shou.edu.cn

通信作者：陈明(1966—)，男，教授，博士，主要从事农业溯源、农业信息技术和食品冷链物流智能化技术研究，E-mail：mchen@shou.edu.cn

independently managed through private channels, effectively avoiding the impact of external traceability operations on it, thus improving the security and controllability of enterprise private data. At the same time, the model can adapt to organizational structure changes, business expansion and other uncertainties in the process of enterprise development, and had good flexibility and scalability. The experimental results showed that the system can still achieve a throughput of 300 transactions/s after the introduction of the security access control model. While improving the system's security and privacy protection capabilities, it had no significant impact on the system performance.

Key words: blockchain; HTSACM; dual-channel; private data collections

0　引言

食品安全问题历来是社会和消费者关注的焦点[1],尤其是在水产品领域。由于水产品对温度和卫生条件要求严格,运输和存储不当容易导致变质和污染[2]。近年来,频发的食品安全事件不仅影响了公众健康,也对水产品行业的声誉和市场信任度造成了严重冲击。因此保障水产品质量安全至关重要,各国对水产品的质量和安全标准提出了更加严格的要求[3],消费者也希望能够准确追溯水产品的来源和加工过程[4]。

危害分析与关键控制点(HACCP)提供了一种以预防为主、贯穿整个生产流程的管理体系,可以更有效地降低食品质量安全风险。2005 年,我国国家标准化管理委员会发布了水产品 HACCP 计划国家标准 GB/T 19838—2005《水产品危害分析与关键控制点(HACCP)体系及其应用指南》,建立规范的水产品 HACCP 体系,为水产品加工行业食品安全提供了保障[5]。很多学者基于 HACCP 计划质量安全监控开展了多角度理论和应用研究。针对国标中的生食牡蛎 HACCP 计划进行本体语义建模研究,丰富本体知识库[6]。通过潜在失效模式及后果分析,定量确定水产品 HACCP 计划的关键控制点[7]。提出农产品区块链溯源系统数据上链机制的改进方法,保证链上 HACCP 数据可信度[8]。针对巴氏杀菌蟹肉增强 HACCP 计划,构建可信可视溯源模型,提高溯源数据可读性[9]。基于洁蛋全产业链流程分析,构建洁蛋 HACCP 计划,并建立全产业链溯源平台[10]。

溯源的前提是数据访问。数据信息化是数据访问的基础,它作为安全监控的重要手段,为溯源系统提供高效、透明、可靠的数据支撑。由于区块链具有去中心化、不可篡改、透明性、可追溯[11]等特点,区块链技术已在溯源系统中广泛使用。出现了基于以太坊和智能合约的大豆跟踪和追溯模型[12],基于区块链和边缘计算的水稻原产地溯源模型[13],基于区块链的河豚供应链溯源优化模型[14]等各类溯源模型。聚焦到水产品溯源领域,通过溯源,在企业、消费者和监管部门之间的信息共享不仅能有效提高溯源系统效率,还能保障水产品质量[15]。然而,生产信息的公开和共享却对企业内部隐私数据的安全性提出了更高要求。这就需要在保障必要数据透明化的前提下,实现对隐私数据的保护。

溯源系统用户跨度很大,对应的溯源数据也应具有不同层次的可见性。其中针对企业内部的敏感数据,需要作为隐私数据进行保护。针对这类数据的保护问题,已有学者从访问控制角度开展了研究。有研究结合区块链和密文策略属性加密(CP-ABE)提出安全可信的农产品溯源体系[16]。CP-ABE 在确保链上数据机密性的同时,实现了数据的细粒度访问控制[17],但这种方法加解密计算复杂度高,性能开销大。还有研究使用智能合约实现基于角色的访问控制(RBAC)模型[18]和基于属性的访问控制(ABAC)模型[19]。RBAC 将角色与权限关联,权限分配灵活[20],但是其存在访问控制颗粒度较粗、无法动态调整权限等问题[21],而 ABAC 则克服了 RBAC 的缺点,实现了细粒度访问控制,并且支持动态调整访问策略[22]。相比之下,RBAC 和 ABAC 由于无须进行加解密计算,产生的性能负载较小[23],更适合数据量大的安全监控系统。在轻量化的基础上,ABAC 实现了灵活、动态、细粒度的访问控制,更符合主体类型复杂的监控系统要求。但是,ABAC 模型在与区块链结合时,存在策略可扩展性弱的问题,策略更新只能通过智能合约以追加方式写入区块链[24],导致链上策略数据持续增长,进而影响策略检索效率。另外,现有研究通常将属性存储在链上并通过智能合约进行管理[25],这使得链上用户均能对属性进行修改,虽提高了属性的动态性,但属性的安全性无法得到保证。同时,由于访问控制无法在底层做到数据隔离,企业对于敏感数据上链也存在顾虑。因此如何在区块链中实现高效且安全的访问控制,并对数据链上存储也实现安全性保护,是值得研究的问题。

本文以巴氏杀菌蟹肉 HACCP 计划为例,基于数据的敏感度构建双通道结构,根据数据分级定义数据访问需求,并采用 ABAC 设计 HACCP 溯源系

统的区块链访问控制模型。该模型首先构建由存储敏感数据的内部通道和存储映射数据的外部通道构成双通道存储结构,实现企业敏感数据和可对外的质量溯源数据的隔离,以保障企业隐私数据的安全性。在双通道的基础上,为内、外通道分别设计访问控制模型,定义不同用户的数据访问需求,并设计属性混合存储方式和策略灵活更新机制,在此基础上设计用户属性和数据访问策略,以在溯源系统中实现多角度的企业隐私数据保护。

1 基于 ABAC 的双通道访问控制模型

1.1 HACCP 溯源系统数据访问需求定义

在 HACCP 计划的信息化中,除了满足溯源需求以外,还需关注企业内部监控数据的隐私性保护。由于不同用户的数据访问需求不同,必须对 HACCP 计划的信息化数据进行访问控制。在已有工作的基础上,针对不同类别用户的数据需求和不同数据的安全保护需求,设计不同的数据安全访问策略。

以巴氏杀菌蟹肉 HACCP 计划为例,结合实际生产情况,在 HACCP 体系原理的基础上,对巴氏杀菌蟹肉生产的全过程进行危害分析,确定各个关键控制点(CCP),并以时间、温度等确定关键限值(CL)。关键控制点包括 CCP1 封口、CCP2 巴氏杀菌、CCP3 成品冷藏。对 CCP2 的杀菌时间和温度及 CCP3 的冷藏温度,依照国家标准 GB/T 30947—2024《罐装冷藏蟹肉》,定义数据的操作限值和关键限值,其中操作限值是理想条件下的最优生产温度,关键限值是满足质量安全的生产温度,操作限制与关键限制之间的生产条件满足食品安全要求但有进一步改进的空间。

在巴氏杀菌蟹肉 HACCP 计划的实施中,当 CCP 出现关键限值偏离时,应当及时记录并采取纠偏行动,隔离偏离期间生产的产品并对其进行评估处置,防止不安全的食品进入消费领域。对于符合安全标准的产品,记录纠偏行动后进入下一 CCP;对于不符合安全标准的产品,予以废弃处理,并将其标记为不合格品,定期向用户通报这些信息。

然后,根据操作限值和关键限值划分风险数据等级,并针对用户的身份和权限定义数据访问需求,详见表 1。由此,引入以下定义:

定义 1:基于用户身份类别,根据访问需求,对不同风险等级的原始监控数据,做出可理解性数据呈现,这种从原始的监控数据到可理解数据(合格或者不合格)的变换称为数据映射,对应的可理解数据称为映射数据。

该映射只涉及数据的可理解性转换以及细节数据的屏蔽,是符合业务处理规则的一种合理化表达。

表 1 HACCP 溯源系统数据访问需求

Tab. 1 HACCP traceability system data access requirement

数据特点	数据等级	数据敏感度	内部主体	外部主体
不大于操作限值	0 级数据	低	合格/细节	合格
大于操作限值 & 不大于关键限值	1 级数据	高	合格/细节	合格
大于关键限值	2 级数据	高	合格/细节	不合格

对于消费者、外部企业、监管机构等外部主体来说,确定产品是否符合生产安全标准是溯源的主要目的,因此系统向外部主体展示各级数据的映射结果,这样简化了数据的呈现和理解,同时确保信息的有效传递,并且一定程度上保护了数据隐私。对于企业自身等内部主体来说,0 级数据完全符合质量安全标准,1、2 级数据则反映了不同程度的质量安全风险。因此了解 1、2 级数据的详细信息,有助于企业精细化管理和生产工艺改进。同时,1、2 级数据作为企业隐私保护的重点,可采用私有数据的形式存储以保证数据安全,并设计访问控制模型以在企业内部中实现数据的细粒度访问控制。

1.2 HACCP 溯源系统访问控制模型架构

在溯源系统中,应在满足溯源需求的同时对企业隐私数据实施保护。首先,为不同类别用户定义不同级别数据的可见范围,降低了数据细节被泄露的风险。其次,使用区块链进行数据存储保证了数据的完整性和可信度,并且通过外部通道和内部通道的双通道结构实现内部细节数据和外部映射数据的隔离。最后,使用基于属性的访问模型对数据资源进行访问控制,细粒度的访问控制可以防止内部细节数据被非法或越权访问,能够保证隐私数据的安全性。

根据 HACCP 计划的数据分级和不同类别用户数据可见范围定义,构建溯源系统访问控制模型,如图 1 所示。模型由 4 层构成,自下而上分别为数据预处理层、数据上链层、访问控制层和数据访问层。

(1)数据预处理层

数据预处理层是访问优化的业务基础层,它负责企业本地存储的原始监控数据的分级和映射处理,从而向数据上链层传输经过处理的映射数据和风险数据。

针对本地存储的 HACCP 计划原始风险数据,首先按照表 1 做数据分级处理,区分出高敏感度数据和低敏感度数据,根据数据敏感度选择不同存储形式。原始风险数据仅在内部通道实现数据细节的传输,供企业内部查看和管理之用。所有数据根据

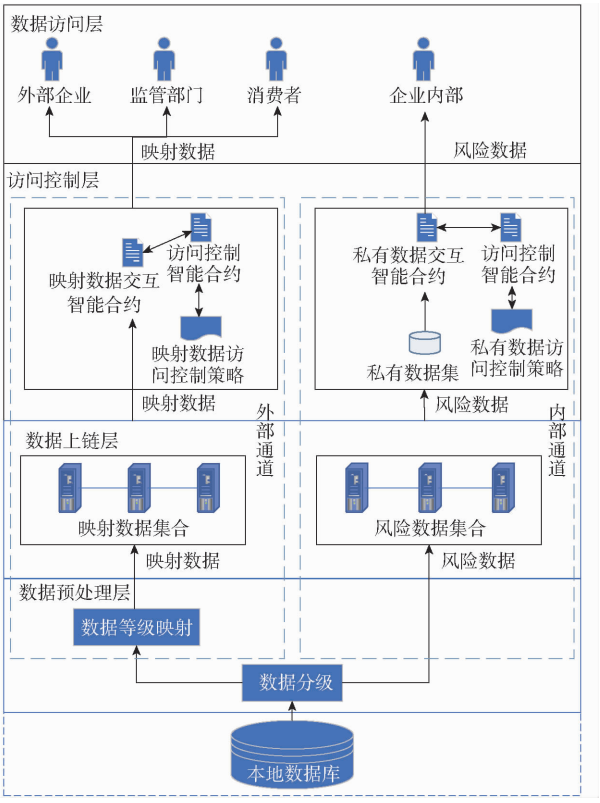

图 1　巴氏杀菌蟹肉 HACCP 计划溯源访问控制模型架构图

Fig. 1　Traceability access control model architecture of pasteurized crab meat HACCP plan

数据等级，做数据映射处理，0 级和 1 级数据映射结果为合格，2 级数据映射结果为不合格。映射后的数据进入外部通道供企业外用户的溯源使用。

(2)数据上链层

数据上链层是访问优化的物理基础层，它负责接收来自数据预处理层上传的映射数据和敏感的细节数据，并实现这些数据的分通道链上存储，然后向访问控制层提供待访问的源数据。

为保护企业的隐私数据，采用 Hyperledger Fabric 中的通道技术将映射数据与细节数据进行隔离存储，设计外部通道和内部通道的双通道架构上链存储模式。其中，外部通道面向消费者、监管部门和外部企业，内部通道则仅面向企业内部各部门。外部通道和内部通道均通过数据上链合约实现数据存储。外部通道链上存储映射数据，内部通道中存储的风险数据，采用访问控制协议加以约束，可实现有控制地内部访问，以保障敏感数据的机密性。

(3)访问控制层

访问控制层是访问优化的核心业务层，它负责对用户的数据访问行为实施严格控制，采用基于属性的访问控制模型以保证隐私数据的安全性。访问控制层接收和处理用户请求，进行实体属性和访问控制策略的匹配判断，判定通过后利用数据交互合约向数据上链层提出源数据请求，并将数据返回给数据访问层。

在访问控制方面，通过对实体属性和策略的分析，设计适用于 HACCP 溯源系统的访问控制模型，并能够在企业组织结构变动时，保持相对稳定的数据保护。通过智能合约技术实现访问控制模型，并且分别部署在外部通道和内部通道上。外部通道中的访问控制主要实现映射数据的细粒度访问控制。内部通道中风险数据采用的私有数据集合存储形式保证了数据在不同组织之间的隐私性，在此基础上，结合访问控制模型为组织内的不同身份用户授予权限，实现内部通道的细颗粒度访问控制。

(4)数据访问层

数据访问层是访问优化的业务服务层，作为用户与溯源系统交互的接口，负责接收用户的访问请求，向访问控制层传递用户请求。并接收访问控制层返回的数据请求结果，反馈给用户。

数据访问层服务的主体有 4 类，包括外部企业、监管部门、消费者和企业内部。其中外部企业、监管部门和消费者仅可访问低敏感度的映射数据，这已经能满足质量安全溯源的需求。而企业内部主要访问风险数据的数据细节，以实现企业内部的及时预警及高效管理。

2　关键技术

2.1　访问控制模型实体、属性设计

2.1.1　实体属性定义

基于属性的访问控制模型本质是实体和策略的集合。实体是访问行为中的所有待控制对象，策略是用来规定访问客体资源需满足的各实体属性要求。实体通过属性描述其特征，并利用属性来定义策略。

HACCP 溯源系统访问模型包含 4 类实体，分别是用户主体、数据客体、访问操作和请求环境，对应的实体属性分别是用户主体属性、数据客体属性、访问操作属性和请求环境属性。其中，参与溯源的用户被定义为用户主体；待溯源的数据被定义为数据客体；待溯源数据的读写访问行为被定义为访问操作；请求根据访问行为进行构建，请求发起的地址和时间被定义为请求环境。

为了确保能够有效地管理不同用户的访问权限，首先需要设计各实体属性，详见表 2。根据 HACCP 溯源系统数据访问需求，企业内部等用户需要访问高敏感度的 1 级和 2 级风险数据，企业外部、监管部门和消费者等用户需要访问低敏感度的映射数据。因此，在实体属性设计时，通过主体属性设计

实现对不同用户的区分,通过客体属性设计实现对数据等级和数据敏感度的区分,两者共同为数据访问控制提供支撑。

为方便描述,将企业内部用户主体根据 Role 属性分为两大类别。Role 属性为第 1 类的主体包括质量控制部门领导、生产部门领导、企业内部监管部门和企业负责人等,Role 属性为第 2 类的主体包括质量控制部门员工、生产部门员工等。

表 2 HACCP 溯源访问控制模型实体属性描述

Tab. 2 Attribute description of access control model entity

实体	属性	描述	取值范围
用户主体	UserID	主体唯一性标识	外部通道主体 ID 以 1 开头 企业内部原主体 ID 以 2 开头 企业内部新主体 ID 以 3 开头 后续数字为从 1 开始递增的整数
	Role	主体所属角色	消费者/监管部门/外部企业/第 1 类/第 2 类
	Relationship	表示主体之间关系	存在隶属关系的用户 ID 属性
	UserTime	主体创建的时间	当前日期,例如 20250101
数据客体	AssetID	数据唯一性标识	从 1 开始递增的整数
	Level	数据等级	0 级/1 级/2 级
	Type	数据类型	Public/Private
	AssetTime	数据上传时间	当前日期,例如 20250101
	Uploader	数据上传者	上传数据的用户 ID 属性
访问操作	Type	操作类型	读/写

用户主体属性设计时,主要考虑对各类用户的特征表达,主要包括:UserID、Role、Relationship 和 UserTime 等 4 个属性。其中,属性 UserID 用以区分不同用户,确保系统能够精确识别每个用户;属性 Role 用以区分用户的角色,确保严格控制用户的访问权限,防止越权;属性 Relationship 用来表达用户的隶属关系,在系统中精确反映用户之间的组织结构;属性 UserTime 则用来记录用户注册的时间,可以在企业结构出现调整时提供访问控制。

数据客体属性设计时,主要考虑对低敏感度数据和高敏感度数据的特征表达,主要覆盖:AssetID、Level、Uploader、Type 和 AssetTime 这 5 个属性。其中,属性 AssetID 用以区分不同数据,确保系统对每条数据实施精确的识别和管理。属性 Level 表示数据的等级,通过数据等级区分数据敏感度,不同级别的数据对应不同的安全要求和访问控制策略,实现对不同敏感度数据的分级管理。属性 Type 是 Level 的补充属性,用以区分内部通道中的风险数据,加强对隐私数据的安全保护。根据数据敏感度将风险数据划分为 Public 数据和 Private 数据,Private 数据采用私有数据集合进行存储。属性 AssetTime 则用来记录每条数据客体的创建时间。属性 Uploader 则表示数据上传者的 UserID 属性。属性 AssetTime 和 Uploader 均服务于动态访问控制。

访问操作实体属性设计时,主要考虑对请求中操作类型的表述。主要设计了 Type 属性,用以区分用户的操作,如读取数据或写入数据的操作。

基于以上对实体属性的定义,企业可以灵活设置不同等级数据的访问控制策略。通过策略设置,企业可以根据各级数据的敏感度和安全需求,精确定义不同用户的数据访问权限,从而确保企业敏感数据的安全性。

2.1.2 属性存储设计

属性作为实现访问控制的重要基础,属性的安全性直接影响访问控制的有效性。同时,在企业的快速发展中,属性的动态性直接影响访问控制的可用性。为了解决以上问题,通过设计混合属性存储形式,以平衡属性的安全性和动态性。

首先根据时效性对属性进行分类。与时间变化具有关联性的为动态属性,与时间变化无关联性的为静态属性。以用户主体属性为例,UserID 和 UserTime 为静态属性,Role 和 Relationship 为实时反映企业内部人事或者组织关系调整的属性,定义为动态属性。静态属性和动态属性分别采用不同形式来存储,如图 2 所示。

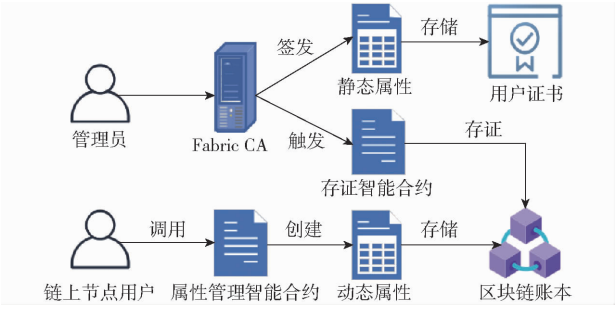

图 2 混合属性存储流程

Fig. 2 Hybrid property storage process

静态属性与用户身份绑定,存储在用户证书中。它通过 Fabric CA 注册并签发,签发后就无法被修改,可以防止属性被篡改,保证属性的安全性。静态属性由管理员进行注册,为防止管理员违规操作,注册时自动触发存证智能合约,将管理员操作以交易形式写入账本,从而实现对管理员行为的监管。

动态属性则通过智能合约进行存储,允许在链上更新属性,满足属性的动态性。最后,结合证书静态属性和链码动态属性实现访问控制,在智能合约

中做组合验证。

2.2　访问控制模型策略设计

2.2.1　外部通道中的 ABAC 策略设计

在 HACCP 溯源访问控制模型中，策略的定义是基于实体属性制定的一系列规则，以决定是否允许溯源用户对映射数据或风险数据执行访问操作。在设计策略时，采用数据的 ID 属性作为标识，为不同数据分别设计访问控制策略。

由于 HACCP 溯源系统的数据采用双通道上链，并且各通道中上链数据的安全保护需求存在差异，因此针对不同通道分别制定相应的策略。

外部通道中存储的是映射数据，外部通道中的主体是消费者、监管部门和外部企业。针对这些主体对映射数据的访问需求，制定的访问控制策略为外部通道策略：允许主体 Role 属性为消费者或监管部门或外部企业且 ID 属性为 1 开头的用户对客体 Level 属性为 0 或 1 或 2 的数据进行读取操作。

当 Role 属性不为消费者、监管部门或外部企业时，对客体的任何类型操作均不被允许。当操作属性非 read 时，主体也都不具有对数据的访问权限。

2.2.2　内部通道中的 ABAC 策略设计

内部通道中存储的数据为风险数据本身。通道中数据的存储形式为私有数据集合，保证数据仅可被企业内部访问。内部通道的主体是企业内部各部门员工和领导。针对这些主体对内部通道数据的访问需求，制定的基础访问控制策略如下：

（1）内部通道策略 1：允许主体 Role 属性为第 2 类且 ID 属性为 2 开头的用户对客体 Level 属性为 0 且客体 Type 属性为 Public 的指定 ID 属性数据进行读取操作。

（2）内部通道策略 2：允许主体 Role 属性为第 2 类且 ID 属性为 2 开头的用户对客体 Level 属性为 1 或 2 且客体 Type 属性为 Private 的指定 ID 属性数据进行读取操作。

策略 1、2 既保证了风险数据的有控制访问，也保证了高敏感数据的不可越权访问。

针对企业组织结构变动时带来的数据访问动态变化问题，制定了如下动态访问控制策略：

（1）内部通道策略 3：允许主体 Role 属性为第 1 类且 ID 属性为 3 开头的用户，在满足主体 Time 属性小于客体 Time 属性的情况下，对客体 Level 属性为 0 且客体 Type 属性为 Public 的指定 ID 属性数据进行读取操作。

（2）内部通道策略 4：允许主体 Role 属性为第 2 类且 ID 属性为 3 开头的用户，在满足主体 Time 属性小于客体 Time 属性的情况下，对客体 Level 属性为 1 或 2 且客体 Type 属性为 Private 的指定 ID 属性数据进行读取操作。

（3）内部通道策略 5：允许主体 Role 属性为第 1 类且 ID 属性为 3 开头的用户，在满足客体 Uploader 属性和主体 Relationship 属性匹配的情况下，对客体 Level 属性为 0 且客体 Type 属性为 Public 的指定 ID 属性数据进行读取操作。

（4）内部通道策略 6：允许主体 Role 属性为第 2 类且 ID 属性为 3 开头的用户，在满足客体 Uploader 属性和主体 Relationship 属性匹配的情况下，对客体 Level 属性为 1 或 2 且客体 Type 属性为 Private 的指定 ID 属性数据进行读取操作。

策略 3、4 允许企业新成员读取自其加入之日起所录入的风险数据，策略 5、6 允许企业新成员在得到授权后对历史风险数据进行读取操作。这 4 个策略在企业组织结构变动时，既保证敏感的历史风险数据不被未授权的人员访问，也可以为新成员或新部门提供必要的数据访问控制支持。

2.2.3　策略更新机制

在以上策略的基础上，为了适应企业快速发展的需求，可以根据企业实时的访问控制需求对策略实施动态调整。

策略的传统管理方法是以事务的形式写入区块链，保证策略的可追溯性[26]，为了提高策略修改的便利性，启用了 Fabric 的状态数据库和账本共同存储策略的方法，具体内容如下：

（1）采用 CouchDB 作为状态数据库，状态数据库中只存储当前最新的策略。策略以键值对的形式保存在状态数据库中，链码通过调用 GetState 和 PutState 来读取和修改策略，实现策略的高效查询和灵活更新。

（2）与传统方式一样，使用区块链账本记录策略创建和更新的历史记录，确保数据的不可篡改性和可追溯性。

为了保证策略更新的原子性，当发起策略更新交易时，会经过模拟执行、生成读写集、背书收集、排序打包、验证，确保交易有效后，才会将交易内容应用到状态数据库并将区块追加到账本中。以上策略更新的具体算法为：

输入：assetID，newPolicy

输出：updatedpolicy

```
1: func updatePolicy(stub shim.ChaincodeStubInterface,
id string, newPolicy string) error {
2: currentState, err := stub.GetState(id) // 查询现有策略
3: var object map[string]interface{}
```

```
4: if err := json.Unmarshal(currentState, &object); err != nil {return fmt.Errorf("could not unmarshal state for key %s: %v", id, err)} //反序列化
5: object["Policy"] = newPolicy //更新策略
6: updatedState, err := json.Marshal(object) //将策略序列化回 JSON
7: if err := stub.PutState(id, updatedState); err != nil {return fmt.Errorf("failed to put state for key %s: %v", id, err)}} //更新状态数据库
```

2.2.4 策略判定优化设计

策略是逻辑运算符和属性组合而成的逻辑表达式。进行策略判定时,通常需要遍历策略集合[27]。当策略数量或属性数量增加时,策略判定时间会明显增加。

策略判定优化的设计思路是:将策略构建为策略树。策略树是对逻辑表达式做解析,将逻辑操作符(如 AND、OR 等)作为根节点和分支节点,将属性的判定条件(取值为 True 或 False)作为叶子节点。进行策略判定时,从策略树的根节点出发,逐层遍历每个叶子节点,当遍历到结果为 True 的叶子节点,则返回判定通过,否则表示判定不通过。通过这种方式,可以有效提高策略判定的效率。

定义 2:在 AND 节点中,若左子树返回 False,则直接跳过右子树评估。在 OR 节点中,若左子树返回 True,则直接跳过右子树评估。这种评估方法称之为短路评估。

定义 3:逻辑表达式采用外层为 OR 逻辑、内层为 AND 逻辑的结构形式进行构建。这种构建方法称之为逻辑表达式的扁平化设计。

为了实现这样的策略优化判定思路,策略树的构建算法为:

(1)对原始策略逻辑表达式进行扁平化设计,以消除冗余嵌套逻辑。

(2)提取公共的判定表达式,减少策略重复判定的时间。

(3)在策略树的根节点和分支节点采用短路评估,在 AND 节点或者 OR 节点中提前终止不必要的子节点评估,优化平均判定性能。

以内部通道中,AssetID 为 11、Level 为 0 且 Type 为 Public 的数据策略为例,为方便描述将逻辑表达式简化为:A = (action = read),R = (role = 1),B1 = (UserID = 21),B2 = (UserID = 31),T = (UserTime < AssetTime),U = (Relationship = Uploader)。原始逻辑表达式为:(A ∧ B1 ∧ R) ∨ [A ∧ B2 ∧ R ∧ (T ∨ U)];扁平化后的策略逻辑表达式为:(A ∧ B1 ∧ R) ∨ (A ∧ B2 ∧ R ∧ T) ∨ (A ∧ B2 ∧ R ∧ U);提取公共条件 A 和 R,简化后的逻辑表达式为:(A ∧ R) ∧ [B1 ∨ (B2 ∧ T) ∨ (B2 ∧ U)],在此表达式基础上构建的策略树如图 3 所示。

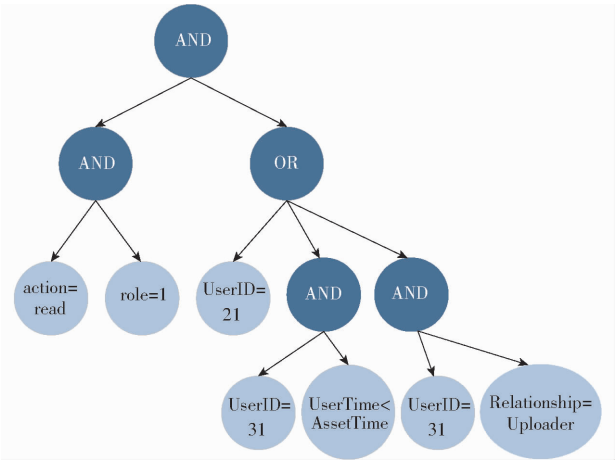

图 3 策略树设计

Fig. 3 Strategy tree design

与原始逻辑表达式相比,优化后的策略树在判定时减少了公共条件 A 和 R 的重复判定,并通过短路评估减少不必要的判断。

3 模型设计

3.1 访问控制逻辑架构设计

在实体属性以及访问控制策略的基础上,为了实现策略和属性的有效管理,维护访问控制模型的整体安全性和可靠性,设计访问控制逻辑,其架构如图 4 所示。该架构由 4 个功能模块组成,分别是:请求处理合约、策略决策合约、Fabric CA 和策略管理合约。

策略管理合约的核心功能是策略的管理,具体包括:创建、维护和更新访问控制策略,并通过智能合约实现这些功能。这些策略规定了满足特定属性要求条件的用户能够访问哪些资源。一旦策略被创建或更新,策略管理合约会将最新的策略信息分发到系统中,确保策略决策合约能够获取最新的访问规则。策略管理合约根据策略决策合约提供的 AssetID,向其返回对应的策略。

Fabric CA 的核心是静态属性管理,具体负责管理和验证用户属性,为策略决策合约提供必要的用户信息。同时,设计 GetUserAttribute 智能合约实现链上动态属性的读取。本模型采用 Fabric CA 作为证书管理的基础,它负责生成、发布和管理数字证书,证书信息用于验证用户在区块链网络中的身份。通过使用私钥对证书内容的哈希值进行签名,任何对证书内容的篡改都会被迅速发现,从而保证了用户属性的可靠性。Fabric CA 根据策略决策合约提供的 UserID,向其返回对应的用户属性。

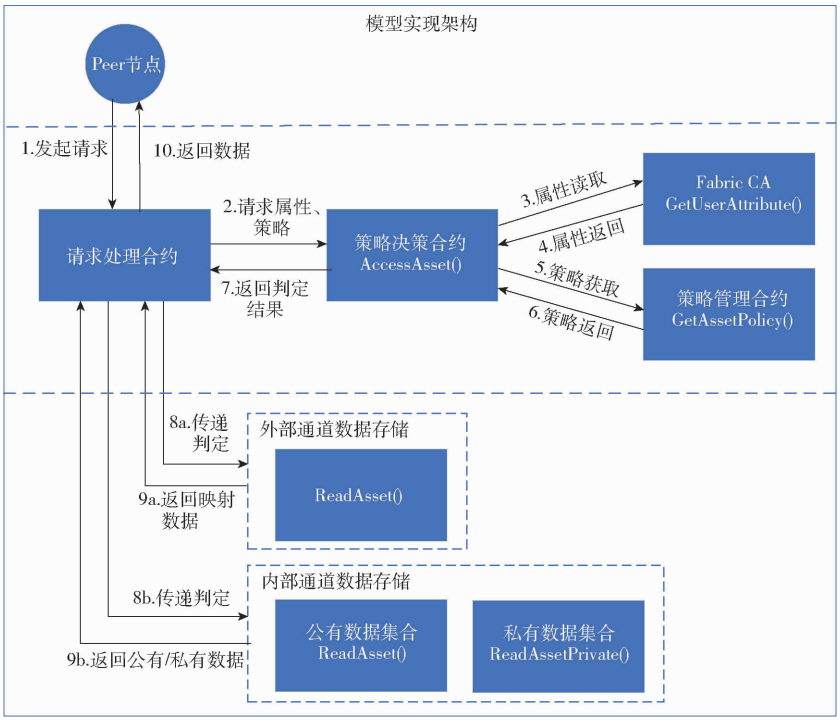

图 4　模型逻辑架构

Fig. 4　Model logical schema

接下来，策略决策合约负责访问控制策略的判断。作为访问控制模型的核心部分，策略决策合约直接决定用户能否访问所请求的资源。策略决策合约接收来自请求处理合约的访问请求，根据访问请求中的 UserID 属性从 Fabric CA 获取用户属性 UserAttribute，根据访问请求中的 AssetID 属性从策略管理合约获取相应访问控制策略 Policy。最后，策略决策合约将所获取的 UserAttribute 与 Policy 进行匹配分析，据此做出是否允许访问的最终决策，并将判定结果返回给请求处理合约。

最后，请求处理合约作为访问控制层与数据上链层之间的中介，接收来自数据访问层的溯源请求，并依据策略决策合约提供的策略判断结果采取行动。如果策略决策合约授权访问，请求处理合约则向数据存储层请求所需的数据并将其返回给数据访问层；如果未获授权，则拒绝访问请求。请求处理合约有效实现了访问控制与溯源等其他业务的有效隔离。其中，内、外通道的数据交互方式存在不同。外部通道中的请求处理合约通过 ReadAsset( ) 读取相应数据返回给 Peer 节点，如图 4 中步骤 8a、9a 所示。而由于内部通道采用私有数据集合的形式存储数据，因此在请求数据时，调用公有数据集合中的 ReadAsset( ) 和私有数据集合中的 ReadAssetPrivate( ) 来分别获取公有数据 Asset( ) 和私有数据 AssetPrivate( )，如图 4 中步骤 8b、9b 所示。

3.2　实验环境

在系统实现中，区块链开发平台采用 Hyperledger Fabric，智能合约的编写使用 Go 语言，区块链网络部署至 Ubuntu 系统。具体的系统配置和软件版本等内容如表 3 所示。

表 3　开发环境

Tab. 3　Development environment description

实验环境	工具及版本号
操作系统	Ubuntu 20. 04. 6 LTS
区块链开发平台	Hyperledger Fabric V2. 5
区块链部署容器	Docker 24. 0. 5
智能合约开发语言	Golang 1. 18
区块链测试工具	Tape 0. 2. 5

3.3　智能合约设计

3.3.1　访问控制智能合约设计

在访问控制智能合约设计中包括策略管理合约、策略决策合约和请求处理合约。策略管理合约主要负责策略的创建和查询，该合约可根据数据 ID 提供已有的对应策略。策略决策合约主要负责策略的判断，该合约可以对用户属性和访问控制策略进行匹配判断，并返回策略判定结果。请求处理合约主要负责访问请求的处理和目标数据的传输，该合约接收策略决策合约的判定结果，若判定结果为允许访问，则向内部通道或外部通道请求数据，并将目标数据返回用户。

(1)策略管理合约

以下是策略管理合约中用于获取指定策略的函数，接收数据 ID 作为参数，并根据数据 ID 在策略库中查询并返回结果。具体算法为：

输入:assetID
输出:policy
1: policyID := "policy_" + assetID//构造策略的键名
2: policyJSON, err := ctx.GetStub().GetState(policyID)//从区块链中读取与策略 ID 对应的数据
3: if policyJSON == nil {return nil, fmt.Errorf("policy for asset %s does not exist", assetID)}//如果没有找到对应策略数据,返回错误提示策略不存在
4: var policy Policy
5: err = json.Unmarshal(policyJSON, &policy)//将JSON 格式的策略数据反序列化为 Policy 结构体
6: return &policy, nil//返回反序列化后的策略数据

(2)策略决策合约

以下为策略决策合约中的核心函数。该函数接收用户 ID 和数据 ID 作为参数,根据用户 ID 获取主体属性,根据数据 ID 获取对应的访问控制策略,然后将策略解析为策略树,通过遍历策略树检查属性是否满足访问控制策略,并返回策略判定结果。具体算法为:

输入:assetID,userID
输出:DecisionResult
1: func (n * AndNode) Evaluate(ctx Context) bool{}//定义 And 节点
2: func (n * OrNode) Evaluate(ctx Context) bool{}//定义 Or 节点
3: func (c * Evaluate) Evaluate(ctx Context) bool{}//定义叶子节点
4: clientID, err := ctx.GetClientIdentity().GetID()//获取当前用户 ID
5: userAttributes, err := s.GetUserAttributes(ctx, clientID)//获取用户属性
6: policy, err := s.GetAssetPolicy(ctx, assetID)//获取与数据 ID 对应的策略
7: func BuildPolicyTree() * PolicyNode{return & PolicyNode}//将策略解析为策略树
8: policyTree = BuildPolicyTree()
9: return &policyTree.Evaluate(context)//遍历策略树检查用户属性是否满足数据访问策略。如满足,返回 True,否则返回 False

(3)请求处理合约

以下为请求处理合约中的核心函数。该函数接收策略决策合约的策略判定结果和数据 ID 作为参数,若策略判定允许访问,则根据数据 ID 获取目标数据,并向用户返回数据。若策略判决为拒绝访问,则提示拒绝访问的信息。具体算法为:

输入:assetID,DecisionResult
输出:Asset
1: flag,err := s.AccessAsset(ctx, assetID)//获取判定结果
2: if flag != true
3: then {return nil, fmt.Errorf("access denied: user does not meet the asset's access policy")}// 若判定结果为拒绝访问,返回错误并提示用户不符合数据的访问策略
4: else {assetJSON, err := ctx.GetStub().GetState(assetID)}//获取数据信息
5: return &asset, nil//返回数据

3.3.2 私有数据集合智能合约设计

首先,在部署私有数据集合智能合约时,通过 collections_config.json 文件定义了公有数据集合 Asset 和私有数据集合 AssetPrivate。其中 Asset 允许 Org1MSP 或 Org2MSP 组织中的任意成员访问该集合的数据,而 AssetPrivate 仅允许 Org1MSP 成员组织访问该集合的数据,即只对企业内部的组织节点可见,如图 5 所示。

```
{
  "name": "Asset",
  "policy": "OR('Org1MSP.member', 'Org2MSP.member')",
  "requiredPeerCount": 1,
  "maxPeerCount": 1,
  "blockToLive":1000000,
  "memberOnlyRead": true,
  "memberOnlyWrite": true,
  "endorsementPolicy": {
   "signaturePolicy":"OR('Org1MSP.member','Org2MSP.member')"
  }
},
{
  "name": "AssetPrivate",
  "policy": "OR('Org1MSP.member')",
  "requiredPeerCount": 0,
  "maxPeerCount": 1,
  "blockToLive":3,
  "memberOnlyRead": true,
  "memberOnlyWrite": false,
  "endorsementPolicy": {
    "signaturePolicy": "OR('Org1MSP.member')"
  }
},
```

图 5 私有数据集合定义

Fig. 5 Private data collection definition

在内部通道中,Asset 中存储的是 0 级风险数据,AssetPrivate 中则存储 1 级和 2 级风险数据,分别设计 ReadAsset 函数用于读取 Asset,ReadAssetPrivate 函数用于读取 AssetPrivate,请求处理合约通过调用这两个函数实现数据交互。具体算法为:

输入:assetID
输出:PrivateAsset
1: log.Printf("ReadAssetPrivateDetails: collection %v, ID %v", collection, assetID)//打印日志,记录当前读取的私有数据集合名称和数据 ID
2: assetDetailsJSON, err := ctx.GetStub().GetPrivateData(collection, assetID)// 从指定的私有

数据集合中读取与数据 ID 对应的私有数据

3：if assetDetailsJSON == nil {return nil,fmt. Errorf ("PrivateData for %v does not exist in collection %v", assetID, collection)} //如果没有找到对应的私有数据,则提示数据不存在

4：var assetDetails * AssetPrivateDetails

5：err = json. Unmarshal (assetDetailsJSON, &assetDetails)

6：return assetDetails, nil//返回私有数据

3.4　安全性分析

溯源访问控制模型(HTSACM)将策略与属性上链存储,并在链上完成访问控制决策过程,继承了区块链的去中心化、不可篡改性与透明性等优势。

(1)去中心化与透明性

模型通过部署于 Fabric 上的分布式智能合约执行访问控制决策,消除了传统中心化授权机制的依赖,实现了访问控制流程的去中心化和公开透明。

(2)不可篡改性

HTSACM 模型中属性与策略数据以链上记录形式进行存储,并仅允许在监管授权下进行更新操作,确保其完整性与一致性。同时,访问控制逻辑由智能合约实现,一旦部署即不可更改或删除,有效保障了控制机制的稳定性。

(3)隐私保护性

为兼顾数据共享与隐私需求,HTSACM 模型引入双通道架构与私有数据集合技术。双通道结构对用户溯源权限进行隔离。在此基础上,通过私有数据集合实现敏感信息的加密存储与定向分发,仅将其哈希值写入账本,原始数据仅在授权节点间传输,从而有效保障了敏感数据的隐私性。

3.5　适用性分析

(1)策略可扩展性分析

HTSACM 模型采用 CouchDB 状态数据库来存储当前最新的策略信息,实现了策略的高效查询,保证了策略的可扩展性。状态数据库查询与全链扫描查询的效率对比如图 6 所示。同时,使用账本对策略的创建与更新进行记录,保障了策略历史数据的不可篡改性与可追溯性。该方法有效支持了企业在动态发展过程中对策略持续迭代与审计追溯的需求,提升了策略管理的效率和可扩展性。

(2)属性安全性和动态性平衡分析

HTSACM 模型将属性划分为静态属性与动态属性两类,并采用混合存储机制加以实现。静态属性 UserID 和 UserTime 经由 Fabric CA 认证签发后,固化于账本之中;动态属性 Role 和 Relationship 则由系统管理员注册管理,并通过存证合约对相关操作

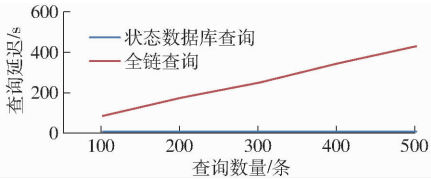

图 6　查询效率对比图

Fig. 6　Query efficiency comparison curves

进行上链记录,确保操作过程的可审计性。该设计在保障属性数据安全性的基础上,有效提升了系统的灵活性与可扩展性,满足了复杂应用场景下对属性动态更新的需求。

3.6　性能分析

在 Hyperledger Fabric 中,不同的区块大小会对吞吐量、延迟等区块链性能指标产生影响。为了保证实验的可对比性和实验变量的唯一性,测试中统一将绝对区块大小设置为 20 MB。在固定其他变量的基础上,使用 Tape 工具分别对访问控制合约和区块链网络进行性能测试。

首先,在固定区块链网络的并发负载的基础上,分别对访问控制合约的交易时间和吞吐量进行测试。对于区块链网络的并发负载,测试中与 Tape 建立 10 个连接,每个连接上模拟 10 个客户端,每个客户端独立向服务器发送请求,即共建立 100 个客户端的并发负载。

在固定并发负载的情况下,测试执行 1 000、2 000、3 000、4 000、5 000 条事务时,执行访问控制合约对交易时间的影响,以检验访问控制合约的效率,实验结果如图 7 所示。根据实验结果可知,在执行不同数量事务下是否部署访问控制对交易时间的影响较小,访问控制合约具有较高的执行效率。

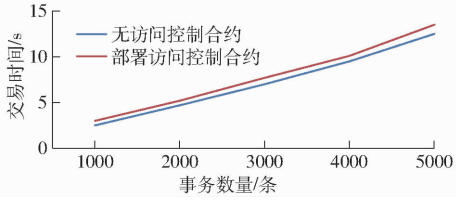

图 7　访问控制合约部署与交易时间关系曲线

Fig. 7　Relationship between deployment of access control contract and transaction time

为检验访问合约的效率,在固定并发负载的情况下,执行 1 000、2 000、3 000、4 000、5 000 条事务时,访问控制合约吞吐量分别为 331、340、352、360、349。在整个实验中,吞吐量均在 300 笔/s 以上,符合实际应用的性能要求。

最后,对改进的策略判定设计进行测试。在固定相同策略的情况下,随机生成 1 000、2 000、3 000、4 000、5 000、6 000 条测试用例,分别测试文献[27]中方法和本文方法判定所用时间,实验结果如图 8

所示。根据实验结果可知,本文方法比文献[27]中方法判定时间缩短 30%。

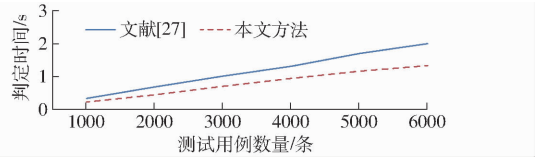

图 8 策略判定时间对比

Fig. 8 Comparison of policy determination time

3.7 原型实现

本研究根据 HACCP 溯源系统访问控制模型,基于 Fabric 区块链实现了访问控制原型系统。图 9a 显示了外部通道消费者和监管部门等根据数据 ID 进行溯源的结果,结果为产品质量合格。图 9b 显示了内部通道企业内部根据数据 ID 进行溯源的结果,结果详细展示每个 CCP 计划的数据。图 9c 显示了进行越权溯源的结果,结果提示用户无权访问该数据。

(a) 外部通道消费者/监管部门溯源

(b) 内部通道企业内部溯源

(c) 越权溯源访问

图 9 HACCP 溯源访问控制原型系统

Fig. 9 HACCP traceability access control prototype system

4 讨论

溯源作为一种有效保障水产品质量安全的手段已被广泛使用,溯源的透明性和真实性为质量安全提供了有力支撑[28-29]。围绕溯源开展的研究或者系统实施也有报道[30-31],然而在多次和相关企业的沟通中发现,企业对于溯源要覆盖企业生产或加工的敏感数据存在安全顾虑。溯源的应用如果不能解决企业的顾虑,无法获取生产一线的质量监控数据的话,产品溯源就无法实施。因此,针对内部通道敏感数据的安全性,也是企业实现进一步质量管理优化的着手点,后续可以在此继续开展深入研究。

本文以巴氏杀菌蟹肉 HACCP 计划为例,结合基于属性的访问控制模型和区块链技术,构建了基于双通道的 HACCP 溯源系统访问控制优化模型,为溯源中企业敏感数据的隐私性保护提供了一种新思路。

5 结论

(1)模型针对不同类型的溯源主体,借助 Hyperledger Fabric 的多通道技术设计了内部通道和外部通道,外部通道存储映射数据,内部通道存储风险数据,实现了数据的存储隔离,企业敏感数据完全不会出现在企业外部溯源的整个通道中。内部通道中的高敏感数据采用私有数据的形式进行存储,只有企业内部的特定权限人员可以访问数据细节,最大限度保障了数据的隐私性。

(2)在外部通道和内部通道的访问控制模型构建过程中,设计了属性混合存储形式和策略灵活更新机制,通过梳理业务需求,定义了访问控制模型属性,针对溯源主体的多样性,设计了主体动态属性和静态属性,并通过“状态数据库 + 账本”的策略更新机制的配合,实时适配企业部门动态调整或变动带来的数据访问权限变化,提升数据随业务调整的实时隐私性同时,也保障了访问的流畅性。

(3)经过测试,在固定并发数的情况下,有访问控制合约和没有访问控制合约的交易时间相近,即访问控制模型对系统资源的占用较低,不会影响使用效能。在不同事务数量的负载下,系统吞吐量基本能达到 300 笔/s,执行操作速度较快,满足多业务处理要求。同时,在高并发负载下,系统性能保持稳定,但性能存在瓶颈,后续可在多用户并发查询优化方面继续研究。本文构建的访问控制模型的功能正常、不同类别用户的溯源需求均可得到满足,也可基本满足溯源系统的业务性能需求。

参 考 文 献

[1] Hoffmann V, Moser C, Saak A. Food safety in low and middle-income countries: the evidence through an economic lens[J]. World Development, 2019, 123: 104611.

[2] Chen J M, Sun R X, Pan C G, et al. Antibiotics and food safety in aquaculture[J]. Journal of Agricultural and Food Chemistry, 2020, 68(43): 11908 - 11919.

[3] Liu F, Rim H. HACCP certification in food industry: trade-offs in product safety and firm performance[J]. International Journal of Production Economics, 2020, 231: 107838.

[4] Yu Z L, Jung D Y. Smart traceability for food safety[J]. Critical Reviews in Food Science and Nutrition, 2022, 62(4): 1 - 12.

[5] Food Agricultural Organization (FAO). Hazard analysis and critical control point (HACCP) system and guidelines for its application: Annex to CAC/RCP 1 - 1969. Rev. 3[S]. 1997.

[6] 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)

[7] 张晨宇, 王伟, 陈志松, 等. 基于 HACCP 和 FMEA 的水产品冷链物流全流程优化[J]. 包装工程, 2023, 44(9): 254 - 264.
Zhang Chenyu, Wang Wei, Chen Zhisong, et al. Full-process optimization of aquatic product cold chain logistics based on HACCP and FMEA[J]. Packaging Engineering, 2023, 44(9): 254 - 264. (in Chinese)

[8] 李佳利, 陈宇, 钱建平, 等. 融合 HACCP 体系的农产品区块链追溯系统精准上链机制改进[J]. 农业工程学报, 2022, 38(20): 276 - 285.
Li Jiali, Chen Yu, Qian Jianping, et al. Improvement of precise on-chain mechanism for agricultural product blockchain traceability system integrated with HACCP[J]. Transactions of the CSAE, 2022, 38(20): 276 - 285. (in Chinese)

[9] 葛艳, 郑珂亦, 邹一波, 等. 增强 HACCP 计划的可信可视溯源应用研究[J]. 农业机械学报, 2023, 54(11): 385 - 396, 411.
Ge Yan, Zheng Keyi, Zou Yibo, et al. Enhanced credible visual traceability application research based on HACCP plan[J]. Transactions of the Chinese Society for Agricultural Machinery, 2023, 54(11): 385 - 396,411. (in Chinese)

[10] 孙若文, 赵思明, 尤娟, 等. 基于 4M1E 和 HACCP 的洁蛋全产业链安全控制系统设计与实现[J]. 中国食品学报, 2022, 22(10): 438 - 449.
Sun Ruowen, Zhao Siming, You Juan, et al. Design and implementation of clean egg whole-industry-chain safety control system based on 4M1E and HACCP[J]. Journal of Chinese Institute of Food Science and Technology, 2022, 22(10): 438 - 449. (in Chinese)

[11] 葛宏义, 吴旭阳, 蒋玉英, 等. 基于区块链技术的粮油食品溯源研究进展及展望[J]. 农业工程学报, 2023, 39(5): 214 - 223.
Ge Hongyi, Wu Xuyang, Jiang Yuying, et al. Research progress and prospect of grain and oil food traceability based on blockchain technology[J]. Transactions of the CSAE, 2023, 39(5): 214 - 223. (in Chinese)

[12] Salah K, Nizamuddin N, Jayaraman R, et al. Blockchain-based soybean traceability in agricultural supply chain[J]. IEEE Access, 2019, 7: 73295 - 73305.

[13] 孙传恒, 袁晟, 罗娜, 等. 基于区块链和边缘计算的水稻原产地溯源方法研究[J]. 农业机械学报, 2023, 54(5): 359 - 368.
Sun Chuanheng, Yuan Sheng, Luo Na, et al. Traceability method of rice origin based on blockchain and edge computing[J]. Transactions of the Chinese Society for Agricultural Machinery, 2023, 54(5): 359 - 368. (in Chinese)

[14] 陈明, 孙浩, 邹一波, 等. 基于区块链的河豚供应链可信溯源优化研究[J]. 农业机械学报, 2022, 53(9): 295 - 304.
Chen Ming, Sun Hao, Zou Yibo, et al. Optimization research on credible traceability of pufferfish supply chain based on blockchain[J]. Transactions of the Chinese Society for Agricultural Machinery, 2022, 53(9): 295 - 304. (in Chinese)

[15] 葛艳, 黄朝良, 陈明, 等. 基于区块链的 HACCP 质量溯源模型与系统实现[J]. 农业机械学报, 2021, 52(6): 369 - 375.
Ge Yan, Huang Chaoliang, Chen Ming, et al. Model and system implementation of blockchain-based HACCP quality traceability[J]. Transactions of the Chinese Society for Agricultural Machinery, 2021, 52(6): 369 - 375. (in Chinese)

[16] Zhang G F, Chen X, Feng B, et al. BCST - APTS: blockchain and CP - ABE empowered data supervision, sharing, and privacy protection scheme for secure and trusted agricultural product traceability system[J]. Security and Communication Networks, 2022, 2022: 2958963.

[17] Guo J T, Yu H Y, Zhang X Q, et al. Blockchain-based digital rights management scheme via multi-authority ciphertext-policy attribute-based encryption and proxy re-encryption[J]. IEEE Systems Journal, 2021, 15(4): 5233 - 5244.

[18] Kamboj P, Khare S, Pal S. User authentication using blockchain based smart contract in role-based access control[J]. Peer-to-Peer Networking and Applications, 2021, 14(5): 2961 - 2976.

[19] Zhang Y Y, Miyabe Y, Sato M, et al. Attribute-based access control for smart cities: a smart-contract-driven framework[J]. IEEE Internet of Things Journal, 2021, 8(8): 6372 - 6384.

[20] Cruz J P, Kaji Y, Yanai N. RBAC - SC: role-based access control using smart contract[J]. IEEE Access, 2018, 6: 12240 - 12251.

[21] 张建标, 张兆乾, 徐万山, 等. 一种基于区块链的域间访问控制模型[J]. 软件学报, 2021, 32(5): 1547 - 1564.
Zhang Jianbiao, Zhang Zhaoqian, Xu Wanshan, et al. Inter-domain access control model based on blockchain[J]. Journal of Software, 2021, 32(5): 1547 - 1564. (in Chinese)

[22] 谢绒娜, 李晖, 史国振, 等. 基于区块链的可溯源访问控制机制[J]. 通信学报, 2020, 41(12): 82 - 93.
Xie Rongna, Li Hui, Shi Guozhen, et al. Blockchain-based traceable access control mechanism[J]. Journal on Communications, 2020, 41(12): 82 - 93. (in Chinese)

[23] Liu H, Han D Z, Li D. Fabric - IoT: a blockchain-based access control system in IoT[J]. IEEE Access, 2020, 8: 18207 - 18218.

[24] 冯鑫昊, 李雷孝, 刘东江, 等. 面向区块链数据共享的访问控制研究综述[J/OL]. 计算机科学与探索, 2025 - 04 - 10. http://kns.cnki.net/kcms/detail/11.5602.TP.20250410.1125.002.html.
Feng Xinhao, Li Leixiao, Liu Dongjiang, et al. Survey on access control for blockchain data sharing[J/OL]. Journal of Frontiers of Computer Science and Technology, 2025 - 04 - 10. http://kns.cnki.net/kcms/detail/11.5602.TP.20250410.1125.002.html. (in Chinese)

[25] 杨信廷, 李金辉, 罗娜, 等. 基于属性访问控制模型的果蔬跨链追溯系统设计与实现[J]. 农业机械学报, 2023, 54(12): 376 - 388.
Yang Xinting, Li Jinhui, Luo Na, et al. Design and implementation of cross-chain traceability system for fruits and vegetables based on attribute access control model[J]. Transactions of the Chinese Society for Agricultural Machinery, 2023, 54(12): 376 - 388. (in Chinese)

[26] 刘敖迪, 杜学绘, 王娜, 等. 基于区块链的大数据访问控制机制[J]. 软件学报, 2019, 30(9): 2636 - 2654. DOI: 10.13328/j.cnki.jos.005771.
Liu Aodi, Du Xuehui, Wang Na, et al. Blockchain-based access control mechanism for big data[J]. Journal of Software, 2019, 30(9): 2636 - 2654. DOI: 10.13328/j.cnki.jos.005771. (in Chinese)

[27] 叶进, 庞承杰, 李晓欢, 等. 基于区块链的供应链数据分级访问控制机制[J]. 电子科技大学学报, 2022, 51(3): 408 - 415.
Ye Jin, Pang Chengjie, Li Xiaohuan, et al. Graded access control mechanism for supply chain data based on blockchain[J]. Journal of University of Electronic Science and Technology of China, 2022, 51(3): 408 - 415. (in Chinese)

[28] Galvez J F, Mejuto J C, Simal-Gandara J. Future challenges on the use of blockchain for food traceability analysis[J]. Trends in Analytical Chemistry, 2018, 107: 222 - 232.

[29] Diamantidis K, Papakostas G, Alexakis T, et al. Blockchain in agriculture traceability systems: a review[J]. Applied Sciences, 2020, 10(12): 4113.

[30] 刘双印, 雷墨鹭兮, 徐龙琴, 等. 基于区块链的农产品质量安全可信溯源系统研究[J]. 农业机械学报, 2022, 53(6): 327 - 337.
Liu Shuangyin, Lei Moyixi, Xu Longqin, et al. Trusted traceability system for agricultural product quality and safety based on blockchain[J]. Transactions of the Chinese Society for Agricultural Machinery, 2022, 53(6): 327 - 337. (in Chinese)

[31] Wang S P, Li D Y, Zhang Y L, et al. Smart contract-based product traceability system in the supply chain scenario[J]. IEEE Access, 2019, 7: 115122 - 115133.