计算机科学
COMPUTER SCIENCE

基于区块链的可搜索属性加密技术应用综述

兰亚杰, 马自强, 陈嘉莉, 苗莉, 许新

引用本文

兰亚杰, 马自强, 陈嘉莉, 苗莉, 许新. 基于区块链的可搜索属性加密技术应用综述[J]. 计算机科学, 2024, 51(6A): 230800016-14.

LAN Yajie, MA Ziqiang, CHEN Jiali, MIAO Li, XU Xin. Survey on Application of Searchable Attribute-based Encryption Technology Based on Blockchain [J]. Computer Science, 2024, 51(6A): 230800016-14.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.230800016

基于区块链的可搜索属性加密技术应用综述

兰亚杰[1,2]　马自强[1,2]　陈嘉莉[1,2]　苗　莉[1,2]　许　新[3]
1 宁夏大学信息工程学院　银川 750021
2 宁夏大数据与人工智能省部共建协同创新中心　银川 750021
3 清华大学电子工程系　北京 100084
(yajielan@stu.nxu.edu.cn)

摘　要　随着信息共享的蓬勃发展,数据隐私安全问题逐渐凸显,催生了区块链技术和可搜索属性加密技术的迅速发展。区块链作为一种去中心化、不可篡改的技术,保障了搜索数据的安全性和完整性,可搜索属性加密技术可以有效地防止非法用户的访问查询。然而随着数据规模和复杂性的增加,出现了检索效率低、查询结果验证复杂、属性权限分发困难等问题。首先,针对以上问题,分别总结了基于区块链的可搜索加密技术、基于区块链的属性加密技术以及基于区块链的可搜索属性加密技术应用的研究现状。其次,对三者之间的优势和侧重点进行了比较分析。最后,重点总结了基于区块链的可搜索属性加密技术在关键字检索、属性权限管理以及数据完整性验证方面的应用,以及所面临的问题和挑战。希望为实现更安全、高效、去中心化的数据存储与共享提供更加安全的技术应用支持。

关键词:区块链;属性加密;可搜索加密;隐私保护;数据共享
中图分类号　TP309.2

Survey on Application of Searchable Attribute-based Encryption Technology Based on Blockchain

LAN Yajie[1,2],MA Ziqiang[1,2],CHEN Jiali[1,2],MIAO Li[1,2] and XU Xin[3]
1 School of Information Engineering,Ningxia University,Yinchuan 750021,China
2 Colaborative imnovaton Center for Ningxia Big Data and Artificial Inteligence Co-founded by Ningxia Mumicinality and Mimistrvy of Education,Yinchuan 750021,China
3 Department of Electronic Engineering,Tsinghua University,Beijing 100084 China

Abstract　With the vigorous development of information sharing,the problem of data privacy security has gradually become prominent,which has spawned the rapid development of blockchain technology and searchable attribute encryption technology. As a decentralized and immutable technology,blockchain ensures the security and integrity of search data,and searchable attribute encryption technology effectively prevents illegal users from accessing queries. However,with the increase of data size and complexity,there are some problems,such as low retrieval efficiency,complicated query result verification,and difficult distribution of attribute permissions. Firstly,in view of the above problems,the research status of the application of blockchain-based searchable encryption technology,blockchain-based attribute encryption technology and blockchain-based searchable attribute encryption technology is summarized respectively. Secondly,the advantages and emphases of these three are compared and analyzed. Finally,the paper focuses on the application of blockchain-based searchable attribute encryption technology in keyword retrieval,attribute permission management and data integrity verification,as well as the problems and challenges faced. It also hopes to provide more secure technical application support for more secure,efficient and decentralized data storage and sharing.

Keywords　Blockchain,Attribute encryption,Searchable encryption,Privacy protection,Data sharing

随着移动互联网的飞速发展,海量数据的产生、存储和传输变得越来越普遍。数据安全和隐私保护成为了亟待解决的热点问题。基于区块链的可搜索属性加密技术可以提高数据安全性和隐私保护的能力,有效防止在搜索过程中数据被恶意攻击者窃取、篡改、泄露等风险,此外,还可以提高数据的利用效率,实现对加密数据的快速搜索和查询。本文将概述基于区块链的可搜索属性加密技术的研究进展,并与传统可搜索属性加密方案进行对比,阐述其主要特点、优势和局限性。

属性加密[1](Attribute-Based Encryption)是一种高度灵活的加密方法,它允许数据拥有者根据用户的属性或角色对

基金项目:宁夏回族自治区重点研发计划一般项目(2022BDE03008);宁夏回族自治区重点研发计划引才专项(2021BEB04047);宁夏自然科学基金一般项目(2021AAC03078)
This work was supported by the Ningxia Hui Autonomous Region Key Research and Development Plan General Project(2022BDE03008),Ningxia Hui Autonomous Region Key Research and Development Plan Special Talent(2021BEB04047) and Ningxia Natural Science Foundation General Project(2021AAC03078).
通信作者:马自强(maziqiang@nxu.edu.cn)

数据进行加密。这种加密方式有助于实现精细化的访问控制，避免了传统加密方法中对称密钥和公钥加密的限制。属性加密可分为基于密钥策略(Key-Policy ABE，KP-ABE)和基于密文策略(Ciphertext-Policy ABE，CP-ABE)两种类型。KP-ABE中，密钥是根据用户的属性生成的，而加密策略嵌入在密文中；CP-ABE则相反，密钥包含访问策略，而属性嵌入在密文中。这两种类型的属性加密各具优势，可以根据不同的应用场景进行选择。ABE在保护数据的同时，提供了灵活的访问控制机制，使得只有满足指定属性条件的用户才能够解密和访问数据。

可搜索加密技术[2](Searchable Encryption)侧重于提供隐私保护和功能性的平衡解决方案。可搜索加密允许用户使用安全索引技术实现高效的搜索功能。可搜索加密技术分为对称可搜索加密(Symmetric Searchable Encryption，SSE)和公钥可搜索加密(Public Key Searchable Encryption，PEKS)。前者依赖于一对对称密钥，适用于单一或固定数量的数据场景，后者基于公钥加密体制，适用于多个数据场景。将ABE和SE算法应用于区块链环境可以实现数据的安全访问和高效检索。区块链技术具有去中心化、可追溯和不可篡改的特点，可以验证搜索数据的完整性和真实性。区块链智能合约结合ABE算法，可以提供更为灵活的的访问控制机制，使得只有满足指定属性条件的用户才能够解密和访问数据，保证了数据的安全共享。

综上所述，基于区块链的可搜索属性加密技术的发展为敏感隐私信息的保护与共享提供了一个有效的解决方案。本文将对基于区块链的可搜索加密技术、基于区块链的属性加密技术以及基于区块链的可搜索属性加密技术应用3个方面的研究现状进行分析和梳理。

本文的主要贡献包括3个方面：

1)通过概括已有文献的主要研究成果和观点，分析了基于区块链的可搜索属性加密技术应用研究现状和发展趋势，为相关研究提供基础和背景知识。

2)通过对已有文献的评估和分析，梳理了基于区块链的可搜索加密技术、基于区块链的属性加密技术、基于区块链的可搜索属性加密技术之间的联系与差异，对现有的多关键字搜索、多权限可撤销访问控制、属性访问策略隐藏等技术进行了分析和比较。

3)通过对已有文献的分析和比较，总结了基于区块链的可搜索属性加密技术应用面临的问题与挑战。

1 相关工作

近年来，基于区块链的可搜索属性加密技术取得了一定的研究成果。研究者们提出了许多方案，以提高ABE和SE在区块链环境中的效率、可扩展性和隐私保护能力。这些研究成果在物联网、医疗数据共享[3]、金融(DeFi)[4]等领域得到了广泛应用。基于区块链的可搜索属性加密技术使用基于块结构加密，实现了更有效的数据处理和属性匹配，如属性撤销(允许删除对特定加密属性的访问)和多用户多权限访问控制(允许管理具有不同权限的多个用户对加密数据的访问)，以及利用隐藏访问策略的方案实现更为隐私的访问控制保护。然而，基于区块链的可搜索属性加密技术应用仍面临诸多挑战，如计算复杂度与通信开销高、存储空间和传输效率低、属性管理混乱等，还需要进一步的研究与创新。

为了应对以上问题，相关学者进行了大量的工作。以下是对现有基于区块链的可搜索属性加密相关综述的总结。

Al-Dahhan等[5]综述了属性加密技术面临的一些障碍，如属性撤销和属性管理问题，分析了现有的单授权和多授权CP-ABE方案，研究了权限撤销问题，但未对动态变化的属性撤销问题以及属性的分配管理问题进行讨论总结，其次没有考虑到区块链对数据隐私保护的影响。Wang等[6]针对经典的ABE方案在效率、安全性等方面存在的问题，从效率提升、策略隐藏、权限撤销、安全性增强等方面进行了探讨，提出了属性加密技术与区块链技术相结合的方案，在保证链上数据安全性的同时实现了细粒度的访问控制的可能。Chaudhari等[7]综述了在云计算环境中进行数据共享时，存在数据被篡改的问题，采用属性加密技术，将云计算环境下的数据共享方案修改为基于密钥策略的加密方案，再将其修改为基于密文的加密方案，最后再将其转换为基于文件层次的密文加密方案，利用层次结构和属性匹配，提供访问控制。How等[8]综述了大多数传统可搜索加密方案的缺点，例如搜索结果的可验证性，分析了现有基于区块链的可搜索加密方案的特点，如安全性和效率，以及基于区块链的可搜索加密方案的潜在漏洞，并讨论了区块链解决了服务器和客户端之间的可验证性和公平支付问题，分析了传统关键字搜索算法只考虑单个关键字的匹配。但作者没有总结如何有效地处理多个关键字的查询。然而随着数据集规模的扩大，结合语义的多关键字检索会成为未来的主要发展方向。Varri等[9]综述了云服务器中不同SE方案，给出了SE方案的分类，介绍了对称可搜索加密、公钥可搜索加密和基于属性的可搜索加密方案，并从索引结构和搜索功能两个方面对这些方案进行了详细的讨论，同时从安全性和性能两个方面对各种可搜索加密方案进行了比较分析，最后讨论了可搜索加密方案面临的挑战、未来发展方向和应用前景，但是没有考虑到云服务器在进行密钥托管以及数据检索过程中存在单点攻击的问题。

综上，在属性加密的综述中，未对动态变化的属性撤销问题和属性的分配管理问题进行分析总结。此外，区块链等分布式服务器的发展，对数据的隐私保护也起到了关键性的作用。在可搜索加密的综述中，针对传统的单关键字搜索算法进行了评述，但没有涉及到随着数据集规模的扩大，对处理多个关键字的查询的分析。结合语义的多关键字检索也将成为未来的主要发展方向。

本文从“基于区块链的可搜索属性加密技术”出发，概述了基于区块链的可搜索加密技术应用发展现状，对比了单关键字和多关键字搜索的搜索效率，以及随着数据规模的增大结合其他技术的多关键字搜索方案，总结了基于区块链的可搜索加密方案结果的完整性验证；并讨论了基于区块链的属性加密技术结合方案，分别从多权限动态撤销访问控制、访问策略隐藏、属性分配管理3个方面进行了对比概述；总结了基于区块链的可搜索属性加密技术应用发展现状，对比了基于区块链的可搜索加密以及基于区块链的属性加密；最后指出了当前基于区块链的可搜属性加密技术应用面临的挑战与问题。

本文第2章对区块链、属性加密、可搜索加密的背景知识进行了介绍；第3章分别从基于区块链的可搜索加密、基于区块链的属性加密、基于区块链的可搜索属性加密3个方面

进行了总结;第 4 章总结了基于区块链的可搜索属性加密的问题与挑战;最后总结全文并展望未来。

2 相关知识

2.1 属性加密技术

属性加密技术是一种公钥加密技术,它允许用户使用一组属性来定义访问控制策略,并根据这些属性来加密和解密数据。在 ABE 中,每个用户都预先定义一组属性,数据也会被赋予一个或多个属性,这些属性可以是任何类型,如用户的身份、所在的组织或用户的位置。ABE 提供了更为灵活的数据访问控制方式,ABE 技术分为两类:基于密钥策略(KP-ABE)和基于密文策略(CP-ABE)。基于策略的 ABE 将属性组织成一个策略集合,然后将这个策略集合作为访问控制策略,用于加密和解密数据。基于密文的 ABE 则将属性直接与密钥相关联,只有当密钥数据中的属性相匹配时才能解密数据。

属性加密方案包括以下 4 个阶段。

1)Setup 阶段:

输入:安全参数 λ。输出:公共参数 PK 和系统主密钥 MK。

$(PK,MK)\leftarrow Setup(\lambda)$

2)KeyGen 阶段:

输入:公共参数 PK 和系统主密钥 MK,用户属性集合 $attr$。输出:用户密钥 SK。

$SK\leftarrow KeyGen(PK,MK,attr)$

3)Enc 阶段:

输入:公共参数 PK,明文 m,访问策略 $\mathcal{P}$。输出:密文 CT。

$CT\leftarrow Enc(PK,m,P)$

4)Dec 阶段:

输入:用户密钥 SK,密文 CT。输出:明文 m。

$m\leftarrow Dec(SK,CT)$

其中,λ 表示安全参数,PK 表示公共参数,MK 表示系统主密钥,$attr$ 表示用户属性集合,SK 表示用户密钥,m 表示明文,CT 表示密文,$\mathcal{P}$ 表示访问策略。

2.2 可搜索加密技术

可搜索加密是一种允许在加密状态下对数据进行查询的加密技术。在传统的加密方式中,数据被加密后就无法进行搜索和查询,只能解密后再进行操作,而可搜索加密技术能够在不暴露数据明文的情况下,寻找特定的数据。可搜索加密技术通常采用加密索引的方式来实现。加密索引是指将数据进行加密后,生成一组索引数据,这些索引数据可以被用来进行查询,在使用加密索引进行搜索时,用户输入搜索关键字,加密算法会对关键字进行加密,并与索引数据进行比对,找到匹配的索引数据,并将其解密以获取相应的明文数据。

可搜索加密包括以下 4 个阶段。

1)建立索引(Index):

输入:明文集合 $\{m_1,m_2,\cdots,m_n\}$。输出:加密索引 I。

$I\leftarrow Index(\{m_1,m_2,\cdots,m_n\})$

2)加密搜索(Search):

输入:加密索引 I,搜索关键词 w。输出:搜索结果集合 $\{m_i\}$。

$\{m_i\}\leftarrow Search(I,w)$

3)加密插入(Insert):

输入:加密索引 I,明文 m。输出:更新后的加密索引 I'。

$I'\leftarrow Insert(I,m)$

4)加密删除(Delete):

输入:加密索引 I,明文 m。输出:更新后的加密索引 I'。

$I'\leftarrow Delete(I,m)$

2.3 基于区块链的可搜索属性加密技术

区块链技术[10]是一种分布式账本技术,允许在去中心化的网络中多个节点之间进行信息的交换和共享。区块链具有去中心化、不可篡改、透明性等特点,其保证了数据再共享过程中的完整性和可信度,使得交易更加公开、透明和可信,提高了交易的信任度以及交易的效率和速度,增强了对个人隐私的保护。区块链技术最初是因为比特币的交易而设计的,但现在已经被广泛应用于其他领域,例如金融、物联网、医疗行业等。区块链技术的基本原理是将交易数据记录在一个称为“区块”的数据结构中,并将这些区块连接在一起形成一个链式结构,即区块链。每个区块都包含了一些交易数据、时间戳和一个指向前一个区块的哈希值。由于每个区块都包含了前一个区块的哈希值,因此任何一个区块的数据被篡改都会导致后面所有区块的数据发生改变,起到了防篡改的作用。

基于区块链的可搜索属性加密技术是将可搜索属性加密技术与区块链技术相结合的一种技术,它利用区块链的去中心化、不可篡改和可追溯等特点,解决了传统可搜索属性加密技术在数据隐私保护和可信性上存在的问题。

具体而言,基于区块链的可搜索属性加密技术将加密后的数据和访问控制策略存储在区块链上,并通过智能合约实现对数据的访问控制和查询。同时,也可以实现数据安全共享和授权管理,使得数据在保护隐私的同时能够被多个授权方进行访问和利用。

基于区块链的可搜索属性加密技术具有以下特点:

1)高度安全性:基于区块链的可搜索属性加密技术采用多重加密和密码学技术,保证了数据共享的安全性和隐私性,利用区块链的不可篡改和可追溯特点,避免了数据被篡改的风险。

2)去中心化访问控制:基于区块链的可搜索属性加密技术将数据和访问控制策略存储在区块链上,实现了去中心化的访问控制和查询,避免了中心化机构的信任问题,增强了数据的可信度。

3)高效性和可扩展性:基于区块链的可搜索属性加密技术采用分布式存储和共识算法,实现高效的数据处理和交易确认,同时具有可扩展性,可应对大规模数据和访问的需求。

3 基于区块链的可搜索属性加密技术应用

本章从 3 个方面详细介绍基于区块链的可搜索属性加密技术:基于区块链的可搜索加密技术、基于区块链的属性加密技术以及基于区块链的可搜索属性加密技术。

在基于区块链的可搜索加密技术方面,进一步将其划分

为关键字检索和审计可验证两个子领域。关键字检索技术主要关注在保护数据隐私的同时，实现对加密数据的高效检索。而审计可验证技术侧重于确保数据的完整性和可靠性，为用户提供可信赖的数据存储和访问环境。本章对这两个子领域的研究进展、优点及存在的问题进行了详细对比和分析。

在基于区块链的属性加密技术方面，本文将其划分为多权限动态可撤销访问控制、属性访问策略隐藏以及混合加密技术 3 个子领域进行阐述。多权限动态可撤销访问控制技术关注如何在保证数据安全性的前提下，实现对用户权限的动态管理。属性访问策略隐藏旨在进一步提高数据隐私保护水平，避免属性泄露。结合其他加密技术的研究则探讨了如何将属性加密技术与其他加密方法相结合，以实现更加全面和高效的数据保护。本章对这 3 个子领域的研究进展、优点及存在的问题进行了探讨。

在基于区块链的可搜索属性加密技术方面，本文将其划分为多关键字搜索、动态权限可撤销以及完整性验证 3 个子领域。多关键字搜索技术致力于提高加密数据检索的灵活性和准确性，满足用户对多样化检索的迫切需求。动态权限可撤销技术关注如何实现对用户权限的动态调整，以适应不断变化的数据访问需求。完整性验证旨在确保加密数据的完整性和可靠性，为用户提供可信赖的数据访问服务。本章对这 3 个子领域的研究进展、优点及存在的问题进行了系统性的分析和评价。

最后对比分析了这 3 个大方面的技术应用研究，总结了基于区块链的可搜索属性加密技术相较于基于区块链的可搜索加密技术和基于区块链的属性加密技术的优点，同时，指出了当前基于区块链的可搜索属性加密技术应用面临的挑战与问题。

3.1 基于区块链的可搜索加密隐私保护

区块链作为一种分布式、去中心化的技术，已经在多个领域取得了重要的应用。其通过将数据分散存储在网络中的多个节点上，使得数据具有高度的安全性和可靠性。然而，区块链仍然存在一些挑战，例如如何实现数据的高效检索等。为了解决这些问题，可搜索加密技术被引入到区块链中，为其提供了一种有效的解决方案。SE 技术是一种加密方式，它可以在不泄露数据内容的情况下，使得数据可以被检索和查询，同时保证数据的可用性和查询效率。基于区块链的可搜索加密技术结合了区块链和 SE 技术的优点，实现了去中心化的可搜索加密数据存储和查询，本节将从关键字搜索、审计可验证两个方面对基于区块链的可搜索加密技术应用进行概括综述。

3.1.1 关键字搜索

关键字搜索是指通过输入单个或多个特定的关键词，在检索系统中进行查询，获取与这些关键词相关的结果。单关键字搜索难以有效处理多个关键字的查询，并且随着数据规模增大，其难以处理多语义的数据检索。表 1 列出了单关键字搜索和多关键字搜索的搜索结果、范围、方式等的对比结果。

表 1 单关键字搜索与多关键字搜索方案比较

Table 1 Comparison of keyword search and multi-keyword search schemes

	单关键字搜索	多关键字搜索
搜索方式	只能输入单个关键字进行搜索	可以输入多个关键字组合进行搜索
搜索结果	返回包含单个关键字的结果	返回包含多个关键字的结果
搜索精度	精度相对较低，可能会出现不相关的结果	精度相对较高，可以更准确地匹配用户的搜索意图
搜索范围	搜索范围相对较广，可能需要用户进行进一步筛选	搜索范围相对较窄，可以直接返回更符合用户需求的结果
搜索复杂度	搜索复杂度相对较低，用户可以快速进行搜索	搜索复杂度相对较高，需要用户输入多个关键字并进行组合，可能会增加搜索难度
适用场景	适用于用户搜索单个关键字的情况	适用于用户需要更精确搜索结果的情况，尤其是需要同时匹配多个关键字的情况

用户在享受云端数据外包便利的同时，也面临着数据被篡改和泄露的风险，以及数据机密性和完整性的验证，并且还存在验证效率低和查询结果不可控等问题。为此，Du 等[11]提出了一种基于公共和私有区块链的隐私保护可搜索加密方案。该方案在私有区块链中存储加密索引，并将相应的加密文档外包给公共区块链，以减少存储开销和提高数据安全性。Mamta 等[12]提出了适用于典型的 CCPS 系统中个人健康数据的在线存储和检索方案，在区块链技术的帮助下，该方案不受权威的约束，实现了真正的分散，消除了对可信授权的需求，减轻了用户的负担。在此基础上，Niu 等[13]提出了一种基于带辅助输入的区块链的密钥聚合搜索加密（KASE）方案，将基于属性的加密（ABE）与可搜索加密（SE）相结合，实现加密数据的安全数据共享，进而提出了一种新的选择明文攻击（CPA）安全方案，并证明了该方案在决策区间-赫尔曼假设和 Goldreich-Leivin 定理下，能够抵抗密钥泄漏的加密文本攻击（CCA）。另外，Gao 等[14]结合基于密文策略属性的加密、Bloom 过滤器和区块链，提出了一种基于区块链的公平可靠可搜索加密方案（BFR-SE），构造了一个基于属性的可搜索加密模型，提供细粒度的访问控制。但是，仅由单个云服务提供商组成的典型可搜索加密模型不能防止恶意行为。为此，Xu 等[15]提出了一种基于区块链的多云环境下的 DSSE（BDSSE-MC）方案，攻击者不能获得原始文件和搜索结果。在此基础上，Zhang 等[16]提出了一种基于区块链的多云可搜索加密方案，将多个云服务提供商组合在一起，通过一个联盟链将数据链接在一起，将加密文档和索引存储到 IPFS 中，缓解了单个云服务器遭受单点攻击的问题。除此之外，该方案还提供了外包加密数据的多关键字排序检索方案和一个检测文件完整性的验证方案，保证了数据的完整性和安全性。由于医疗数据具有隐私性和敏感性，不同医疗机构之间面临数据共享困难和数据隐私泄露等安全问题。Yang 等[17]提出了一种基于区块链的 EHR 安全存储与共享可搜索代理重加密方案，以防止电子健康记录被篡改和泄露；采用无证书加密和基于身份和类型的代理重加密作为数据共享协议，实现了第三方数据用户对医疗卫生数据的安全访问。

现有的加密方案易受自适应泄漏攻击，不能满足实际应用的检索要求，特别是可搜索公钥加密方案（SPE）。为了能够实现安全高效的关键字搜索，Chen 等[18]设计了一种基于区块链的可搜索公钥加密方案（BSPEFB）。BSPEFB 是一种

分散搜索的公钥加密方案，中央搜索云服务器被智能合约取代。同时，BSPEFB 支持前向和后向隐私，实现隐私保护。然而，传统的 PEKS 方案不能抵抗关键字猜测量子计算攻击，其安全性依赖于密钥的机密性，因此 Xu 等[19]提出了一个基于区块链的后量子公钥可搜索加密方案(PPSEB)。该方案利用基于格的加密原语保证了搜索过程的安全性，实现了前向安全性，避免了医疗信息的密钥泄露；其次，引入区块链技术解决了搜索过程中的第三方不可信问题。针对现有云环境下可搜索加密方案搜索效率和精度低、安全性差等问题，Yang 等[20]提出了一种基于区块链技术的可跟踪、关键字搜索加密方案，以实现用户查询的可追溯性，防止非法用户泄露敏感数据。为了解决现有基于区块链的可搜索加密方案只支持精确关键字搜索的问题，Yan 等[21]提出了一种基于区块链的可搜索加密方案，该方案具有文件动态更新、搜索结果验证、模糊关键字搜索和公平支付等功能。其使用编辑距离来生成模糊关键字集，很大程度上提高了检索的范围。在此基础上，Yang 等[22]设计了一个可靠的智能合约来代替中央云服务器进行密文检索，以确保检索结果的正确性和交易的公平性。另外，作者在模糊关键字的基础上，提出了正向和反向私有模糊多关键字可搜索加密(FBPB-SE)方案，可以同时实现向前和向后的安全性证明。但也存在查询结果准确性不高以及结果歧义的问题。为此，Xu 等[23]设计了一种基于区块链的多关键字可验证可搜索的对称加密方案，使用位图来构建搜索索引，并使用区块链来确保搜索结果的公平验证；将位图和哈希函数相结合，实现了轻量级的多关键字搜索结果验证。大多数现有的排序可搜索加密方案没有考虑外包服务的付费问题。Xu 等[24]提出了一种基于差分隐私和区块链的排序搜索加密方案(DPB-RSE)，将来自拉普拉斯分布的噪音添加到相关性得分中，以扰乱其值。此外，为了提高共享方案的效率和安全问题，Ali 等[25]提出了一种新的基于群论(GT)的二进制弹簧搜索(BSS)算法，由混合神经网络方法组成，并采用同态加密的技术，确保了安全的关键字搜索。表 2 列举了近几年关键字搜索在优化目标、安全性、查询方式、攻击防御等方面的比较。

表 2　可搜索加密技术关键字搜索对比

Table 2　Comparison of keyword search with searchable encryption technologies

类型	相关工作	设计目标	安全性	查询方式	攻击防御	局限性
关键字搜索	Du[28]	优化索引	区块链	单关键字查询	抵御选择关键词攻击	查询效率较低
	Mamta 等[12]	优化查询	区块链	单关键字查询	抵御单点攻击	查询结果的完整性验证
	Gao 等[14]	优化查询	Bloom 过滤器和区块链	单关键字查询	抵御选择关键词攻击	单个云服务器易遭受单点攻击
	Zhang 等[16]	优化索引	多云服务器＋联盟链	单关键字查询	抵御单点攻击	计算开销大、查询效率低
	Yang 等[17]	优化查询	区块链＋基于身份和类型的代理重加密	单关键字搜索	抵御单点攻击	计算开销大
	Chen 等[18]	优化查询	前向和后向隐私保护	多关键字查询	抵御单点攻击	计算复杂度高
	Xu 等[19]	优化查询	后量子公钥加密＋基于格密码加密	多关键字查询	抵御选择关键词攻击、密钥泄露、量子攻击	计算开销大，计算复杂度高
	Yan 等[21]	优化查询	区块链	模糊关键字查询、多关键字查询	抵御选择关键词攻击	查询复杂度高、查询精度低
	Yang 等[22]	优化查询	前向和后向隐私保护	同义词向量拆查询、模糊关键字查询、多关键字查询	抵御抵御选择关键词攻击	计算开销大
	Xu 等[23]	优化索引、优化查询	前向隐私保护	采用位图构建索引、多关键字查询	抵御抵御选择关键词攻击	通信开销大、计算复杂度高
	Xu 等[24]	优化查询	差分隐私、区块链	多关键字查询	抵御抵御选择关键词攻击	计算复杂高
	Ali 等[25]	优化查询	同态加密、区块链	基于群论(GT)的二进制弹簧搜索(BSS)算法		计算开销大，计算复杂度高

3.1.2　审计可验证

审计可验证是指在数据审计过程中，通过使用可验证性技术，确保数据的完整性、可信度和不可篡改性。但是传统的云服务器是半诚实或好奇的，容易遭受单点攻击。本小节对可验证区块链进行了总结。

在现有方案中云服务器通常假设为诚实但好奇的，但现实中可能并非如此，因此，Li 等[26]提出了一种可验证的基于区块链的公钥加密方案，将验证外包给 TrueBit 网络，最大限度地降低了矿工的计算成本。在此基础上，Wang 等[27]提出了一种具有聚合授权和可信撤销的高效验证 SE 方案，数据使用者有权搜索文档并验证搜索结果，通过利用可信执行环境，数据拥有者可以撤销数据使用者的搜索权限，实现了数据拥有者对数据的控制权。

虽然结果验证问题有了解决方案，但是大多数方案都集中在静态环境中，没有考虑动态环境中的结果验证问题，因此，Du 等[28]提出了一种基于可验证区块链的前向和后向隐私方案的可搜索加密算法(VBSEFB)。VBSEFB 支持在动态环境中对云服务器返回的数据进行本地验证，实现了数据所有者对数据用户的访问控制。在此基础上，为了让服务器能够更好地获取动态更新后的数据，以及验证更新后搜索结果的正确性，Guo 等[29]提出了一种基于区块链技术的动态 SSE 方案，并将其应用于底层构建模块，以保持前向安全更新。其次，还采用智能合约来制定验证方案，使更新的结果易于验证。表 3 列举了静态方案和动态方案的特点。

表 3　静态验证和动态验证技术方案

Table 3　Static verification and dynamic verification technical schemes

验证技术	特点	相关工作
静态方案	1)可验证的公钥加密方案，实现了有效的可验证性	Li 等[26]
	2)聚合授权可撤销的高效验证方案，利用可信执行环境实现安全的搜索	Wang 等[27]
动态方案	1)前向安全性的可验证和动态 SSE 构造，采用智能合约实现前向安全更新	Guo 等[28]
	2)前向和后向隐私方案的可搜索加密算法，支持在动态环境中对数据的本地验证以及获取动态更新后的数据	Du 等[28]

以往都是采用对称可搜索公钥加密，然而，现有的带有关

键字搜索(PAEKS)的公钥认证加密方案是基于双线性配对的,导致计算量增大。为了解决这个问题,Du 等[30]提出了一个基于区块链的 PAEKS 方案,该方案支持多关键字查询和完整性验证,并且在决策先知迪菲-赫尔曼(DODH)假设下为 PAEKS 方案提供了安全性证明。可搜索加密是云端存储所必需的重要服务,它可以实现加密云端数据的信息检索功能,同时保护隐私。为了避免隐私数据在共享过程中被伪造、篡改等,Li 等[31]提出了一种基于联盟区块链的数据安全存储与共享方案,AES 和 RSA 加密技术对数据、关键字和数字签名进行加密存储,该方法可以实现数据的高可用性和隐私保护。Yang 等[32]提出了一种基于区块链的电子健康记录数据检索方案,实现了分散网络环境下电子健康记录数据的计算和应用,采用基于属性加密的机制,实现了对云数据的细粒度访问控制,并利用属性签名技术验证了 HER 数据源的真实性。Zhang 等[33]为了保证图像数据的隐私性和可操作性,提出了一种基于区块链和可否认认证加密技术的医学图像数据共享(DASES)搜索加密方案,保证了图像数据的非篡改性和可追溯性。

3.2 基于区块链的属性加密隐私保护

基于区块链的属性加密技术是一种数据加密技术,随着区块链技术的迅猛发展,其在各个领域中的应用越来越广泛。该技术主要是利用区块链技术的不可篡改性和加密算法的安全性,对数据进行多层次的加密和授权,从而保证数据的安全性和隐私性。在基于区块链的属性加密技术中,数据会被分成多个属性,每个属性都有一个相应的密钥,只有拥有属性的用户和设定的属性满足门限值才能够访问数据。这种加密方式不仅能够保证数据的安全性,还具有访问控制的作用,然而,基于区块链的属性加密技术在仍存在一些问题和挑战,如属性的管理与分发、访问策略的泄露等。本节将从多权限动态可撤销访问控制、属性访问策略隐藏以及结合其他加密技术 3 个方面对基于区块链的属性加密技术应用进行综述。

3.2.1 多权限动态撤销访问控制

传统的权限分发集中在单个访问控制中心,容易遭受单点故障攻击,而且权限撤销周期长。多权限动态撤销访问控制引入了多个权限颁发机构,每个机构负责一部分权限管理,避免了单点故障,并可以实时对权限进行撤销管理。本小节主要对多权限访问控制及传统访问控制进行了分析和总结。

现有的基于属性的加密方法中,所有用户属性都由一个中间机构管理,很容易导致单点故障,为此,Qin 等[34]提出了一种基于区块链的多权限访问控制方案 BMAC 来实现数据的安全共享,引入 Shamir 秘密共享方案和许可区块链(Hyperledger Fabric)实现了每个属性由多个权限联合管理,以避免单点故障。针对信息透明度低、交互延迟等问题,Liu 等[35]提出了一种新的基于隐私保护的多权限属性访问控制方案,实现了细粒度的访问控制和灵活的授权方式,即使某些属性权限授权失败,用户的私钥也不会泄露。为了提高访问控制策略效率低下,以及密钥滥用和缺乏灵活性等问题,Guo 等[36]提出了一种基于区块链的可追踪属性的动态访问控制(TABE-DAC)加密方案,该方案支持对恶意泄露私钥用户的可追溯性,动态访问控制可以让数据所有者灵活地更新访问控制策略,进而实现对隐私数据的安全保护。Pournaghi 等[37]采用了区块链和属性加密技术,提出了对医疗数据记录存储的 MedSBA 方案,该方案允许基于一般数据保护规则(GDPR)的细粒度医疗患者数据访问控制。私有区块链在 MedSBA 中用于改善撤销访问的权利。Sharma 等[38]基于区块链和密文策略属性,提出了一种动态用户撤销方法,使用密钥生成算法对数据所有者和属性权限进行注册。其次,数据所有者和属性授权机构将公共信息存储在区块中,并设置访问策略,生成用户的秘密密钥。由于基于属性加密(ABE)和带有关键字搜索的公钥加密(PEKS)在解密和撤销方面存在较高的开销,并且在搜索中存在隐私泄露问题,因此 Yu 等[39]提出了一种高效的可撤销可搜索的多权限 ABE(MA-ABE)方案 ERS-ABE,该方案利用区块链实现基于关键字的搜索和动态用户管理。ERS-ABE 还采用云辅助解密技术来提高物联网设备的效率。此外,Xiao 等[40]为了提高用户撤销操作的灵活性,提出了一种基于密钥策略属性的多重灵活撤销加密方案(MAFR-KP-ABE),以实现分散授权和灵活撤销。为了解决节点退出需要撤销其相应权限并更新全部用户权限的问题,Hongmin 等[41]提出了一种基于区块链的个人数据安全共享方案 BSSPD,BSSPD 支持对特定数据用户的属性级权限撤销,而不会影响其他用户。图 1 给出了多权限动态撤销访问控制的机制。

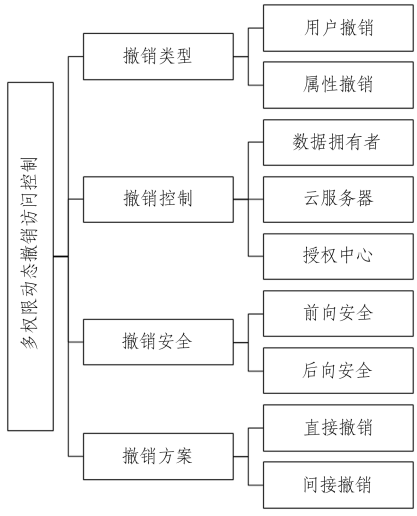


图 1 多权限动态撤销访问控制机制

Fig. 1 Multi-permission dynamic revocation access control mechanism

以上方案主要针对数据用户属性的撤销问题,未涉及数据拥有者对数据的掌握权以及在共享过程中的数据隐私保护问题。医疗资源服务中存在病人的电子健康记录共享困难,以及患者无法掌握其病例使用情况等问题,为此,Yang 等[42]提出了一种基于患者控制和云链协作的多权限属性加密算法(VO-PH-MAABE),用于可验证外包解密和隐藏访问策略的电子病历共享,利用区块链的不可变性来存储验证参数,并利用 Shamir 秘密共享和智能合约来计算跨域管理的属性密钥或令牌,避免了单点故障,并减少了数据用户端的通信和计算开销。Alishehri 等[43]提出了一种基于密文策略属性加密(CP-ABE)算法和区块链技术相结合的细粒度数据访问控制方法,该方案具有相同属性的雾节点联合,最小化了雾节点和云服务器之间的时间延迟和通信开销。远程医疗可提供远程医疗点播(MoD)服务,旨在克服距离障碍,改善偏远农村社区获得医疗服务困难的问题。Guo 等[44]提出了一种基于 ABE

的动态认证与授权的远程医疗系统方案,该方案可以实现对远程医疗系统 MoD 服务更加灵活、高效的动态认证与授权,并且该系统由多个权限共同管理,避免了因内部云端的恶意用户篡改不准确的电子健康记录而导致误诊。传统电子健康记录都是由医院进行控制的,这使得向不同医院寻求医疗建议变得复杂,患者迫切需要拥有对自己医疗数据的管理权,为此,Guo 等[45]提出了一种基于属性多权限签名方案,该方案存在多个权限,没有可信的单一中央权限来生成和分发患者的公私钥,解决了密钥托管泄露问题。表 4 列举了相关工作中撤销类型、撤销控制等的对比。

表 4　多权限动态撤销访问控制方案

Table 4　Multi-permission dynamic revocation access control scheme

相关工作	撤销类型	撤销控制	撤销安全	撤销方案
	用户撤销/属性撤销	数据拥有者/授权中心/云服务器	前向安全/后向安全	直接撤销/间接撤销
Sharma 等[38]	用户撤销	数据拥有者	前向安全	直接撤销
Yu 等[39]	用户撤销	授权中心	前向安全	间接撤销
Xiao 等[40]	用户撤销	授权中心	前向安全	间接撤销
Gao 等[41]	属性撤销	授权中心	后向安全	间接撤销
Qin 等[34]	属性撤销	授权中心	前向安全	间接撤销
Liu 等[35]	属性撤销	授权中心	前向安全	间接撤销
Guo 等[36]	用户撤销	授权中心	后向安全	间接撤销

3.2.2　访问策略隐藏

访问策略隐藏是将访问策略信息进行加密,以防止未经授权的用户访问与解密。本小节主要对用户属性隐私和访问策略隐私进行分析和总结。

随着云存储系统的大规模应用,为了在不安全的环境下保护用户数据的安全,基于属性的访问控制方案被提出。Li 等[46]构造了一个支持隐私保护的 ABAC 方案,该方案可以解决属性系统中用户属性隐私和策略隐私的问题,此外还利用智能合约解决了属性撤销和策略更新问题。目前 ABE 访问控制方案依赖于可信的云服务器,安全性较低。Yang 等[47]提出了一种基于区块链的 ABE 云存储数据访问控制方案,该方案基于密文策略 ABE 算法,支持隐式访问策略,避免了隐私泄露的风险。Yang 等[48]提出了一种基于区块链和混合加密隐藏策略的安全网格数据共享方案,该方案采用多属性授权机制防止合谋攻击,隐藏策略保证用户信息不被泄露。传统的基于密文策略属性的加密方案具有增强明文安全性和细粒度访问控制的特点,然而加密过程需要消耗高性能的计算。为此,Qin 等[49]提出了一个基于区块链和本地差分隐私的可验证 ABE 方案,使用 LDP 在一定程度上扰乱本地原始数据以抵御串通攻击。

然而,现有解决方案在计算开销和计算复杂度方面仍然存在缺陷。Zhang 等[50]提出了一种基于区块链的、带有隐藏策略的基于属性的 SHS 访问控制方案。该方案引入了多个授权机构,避免了单点故障。为了解决医疗行业存储安全、共享可靠、访问控制和隐私保护等问题,Li 等[51]提出了一种基于区块链的 HER 系统——EHRChain,该系统采用基于属性的同态密码来解决上述问题。作者提出了一种改进的密码原语 SHDPCPC-CP-ABE,实现了基于部分密文半策略隐藏和动态权限更改功能;采用参数优化的加性同态 Paillier 密码体制保护了患者隐私。Mittal 等[52]提出了一种两级访问控制技术来解决隐私泄露问题,结合基于密文策略属性加密,使用代理重加密实现安全的数据传输。表 5 列举了相关工作在用户属性隐私、属性策略隐私方面的特点。

表 5　访问策略隐私分类

Table 5　Privacy classification of access policy

隐私保护对象	特点	相关工作
用户属性隐私	智能合约解决了属性撤销和策略更新问题	Li 等[46]
	本地差分隐私的可验证 ABE 方案,扰乱本地原始数据以抵御串通攻击	Qin[49]
	区块链的、带有隐藏策略的基于属性的 SHS 访问控制方案,策略隐藏保护了用户的敏感信息	Zhang[50]
策略隐私	基于区块链的 ABE 云存储数据访问控制方案	Yang[47]
	基于区块链和混合加密的带隐藏策略的安全网格数据共享方案,采用多属性授权机制,隐藏策略了保证私人信息不被泄露	Yang[48]
	采用基于属性的同态密码体制,实现了基于部分密文的半策略隐藏和动态权限更改功能	Li[51]
	采用两级访问控制技术,使用代理重加密来实现安全的数据传输和仅对请求者的匿名性	Mittal 等[52]

3.2.3　混合加密

混合加密是将属性加密和其他加密技术结合起来实现对隐私数据的保护。本小节对基于区块链的属性加密技术结合其他加密技术进行了分析和总结。

为了实现医疗数据的机密性、认证性、完整性,Wang 等[53]提出了一种基于属性密码体制和区块链技术的安全电子病历系统,使用基于属性加密和基于身份加密来加密医疗数据,并使用基于身份签名来实现数字签名。恶意用户通过收集区块链上的交易信息进行数据分析,对用户的隐私造成了潜在风险。Xu 等[54]提出了一种高效的基于区块链的具有属性和同态加密的隐私保护方案,该方案可以实现用户级细粒度的安全访问控制,采用基于属性加密和同态加密两种控制方法减少了用户隐私数据的泄露。Liang 等[55]提出了一个基于联盟区块链的个人数据隐私保护方案,使用改进的 Paillier 同态加密机制加密原始数据,提高了数据的传输效率,并通过链下存储和链上传输协同作用来保证用户数据的隐私安全。Zhang 等[56]将 CP-ABE 算法和 DES 算法结合,设计了一种混合数据加密方案,实现了 1 到 N 的加密数据共享,提出区块链技术下“横向+纵向”方案。同时,Baek 等[57]采用基于密文策略属性的代理重加密方案,提出了一个基于区块链的病历共享框架;采用基于密文策略属性的代理重加密方案,实现了细粒度的访问控制。Ullah 等[58]提供了一个基于区块链的分布式存储共享方案,提供端对端加密和细粒度的访问控制,使用 AES 进行加密,并使用椭圆曲线迪菲-赫尔曼密钥交换协议在数据所有者和用户之间共享密钥。为了解决电子病例患者隐私数据泄露问题,Yuan 等[59]设计了一个三链模型来分层存储病人信息、医务人员信息和病历,采用属性加密技术对密钥和密文路径进行二次加密。He 等[60]在线性秘密共享方案(LSSS)的基础上,提出了一种协同方案,在数据所有者的许可下,可以使用同一组内其他用户的私钥进行协

同解密，降低了计算和存储开销。

在数字化时代，传统的集中式医疗系统和半可信云服务器难以实现隐私保护与数据共享之间的动态平衡。针对这些问题，Zhang 等[61]提出了一种基于双区块链医学数据存储共享方案。对称加密技术与基于密文策略属性相结合，不仅保证了存储安全，而且实现了数据更新的一致性，避免了数据的冗余。尽管基于云的电子健康记录可以解决数据共享和管理中存在的问题，但是容易受到各种恶意攻击。Chen 等[62]提出了基于区块链的细粒度安全电子健康记录共享机制 BF-HS，使用基于密文策略属性加密（CP-ABE）对 EHR 进行加密，匹配索引通过代理重加密进行加密。Chen 等[63]提出了一种实用的基于区块链和分散属性加密的医疗文件共享方案。其利用分散的属性加密技术，对医疗文件进行细粒度访问控制，既保证了文件的隐私性和安全性，又避免了单点故障。Li 等[64]提出了一种基于属性的分层加密方案来实现对医疗数据的访问控制，为了提高用户的查询效率，提出了一种结合跳跃列表和 Bloom 过滤器的区块链查询索引。随着传统病历的数字化，医疗电子病历出现了数据存储和共享等难题。Niu 等[65]提出了一种基于许可区块链的医疗数据共享方案，采用基于密文属性加密来实现对医疗数据的访问控制，在保证患者身份隐私的前提下，采用多项式方程实现了关键字的任意连接。Guo 等[66]提出了一种基于属性加密的支持跨域可搜索数据共享方案，通过关键字策略实现了灵活的密文搜索，以及访问过程中的可追溯性和防篡改性。为了提高医疗数据的检索效率，Su 等[67]基于以太坊构建了两个智能合约，分别为搜索智能合约（SSC）和验证智能合约（VSC），用于将用户的陷门与索引进行匹配，并验证搜索结果的的正确性。为了提高搜索精度，实现了一种只返回 top-k 的排序多关键字搜索，解决了数据共享过程中的隐私保护问题。为了减轻数据计算负担，许多分布式解决方案被提出用于解决集中式服务器数据孤岛问题。Li 等[68]介绍了一种高效的电子病历管理模型——上链分类和下链存储（OLOS），基于格密码的安全关键字搜索属性加密（KS-ABE）方案，减轻了公共分类账本的计算负担，节省了公共云空间，同时保护了跨机构 EMR 的安全共享，并具有抵抗量子攻击的能力。表 6 列出了属性加密技术结合其他加密技术的隐私保护方案。

表 6 属性加密技术结合其他加密技术隐私保护方案

Table 6 Privacy protection schemes of attribute encryption technology combined with other encryption technologies

相关工作	方法	优点	面向场景	缺点
Wang 等[53]	基于属性的加密（ABE）和基于身份的加密（IBE）	具有良好的开放性和透明性	数据共享	容易遭受链接攻击
Xu 等[54]	同态加密	实施细粒度访问控制以及数据缺乏透明度和可审计性	数据共享、访问控制	同态加密计算开销大
Liang 等[55]	Paillier 同态加密机制	提高了数据的传输效率，并通过脱链存储和链上传输协同作用来保证用户的隐私和安全	数据共享、数据存储	加密解密计算开销大
Zhang 等[56]	CP-ABE 算法和 DES 算法混合加密方案	显著降低了密钥管理的复杂度，能够实现加密数据的高效共享	数据共享	混合加密计算开销大
Baek 等[57]	基于属性的代理重加密方案	实现了细粒度的访问控制，在紧急情况下无需患者同意即可共享信息	访问控制、数据共享	容易遭受单点攻击
Ullah 等[58]	高级加密标准（AES）进行加密，并使用椭圆曲线迪菲—赫尔曼密钥交换协议	分散式分布式存储和共享方案，提供端对端加密和细粒度的访问控制	分布式存储、数据共享	计算和处理资源要求较高，性能和效率受到限制
Yuan 等[59]	三链模型来分层加密	降低了系统攻击的风险，解决了单链模型吞吐量低、稳定性差的问题	密钥管理、数据加密存储	系统的复杂度高，性能受到限制
He 等[60]	线性秘密共享方案（LSSS）的基础上，提出了一种实现协同解密功能的协同方案	显著降低了计算和存储开销	数据存储、数据共享	安全性、效率较低，导致秘密的泄露或者损坏
Zhang 等[61]	双区块链方案	保证了数据在云中的安全存储，而且实现了数据更新的一致性和方便性，避免了数据的冗余备份	数据存储、数据共享	易受到恶意攻击、信任管理和服务器之间的不可否认性
Chen 等[62]	代理重加密	基于密文策略属性的加密（CP-ABE）对 EHR 进行加密，索引通过代理重加密进行加密	数据加密存储、数据共享、访问控制	安全性问题，容易存在安全漏洞，可扩展性较差
Chen 等[63]	分散的基于属性的加密技术	保证了文件的隐私性和安全性，又避免了单点故障	数据存储、数据共享	易受到密钥泄露攻击，可信赖性问题
Li 等[64]	基于属性的分层加密方案、结合跳跃列表和 Bloom 过滤器的区块链查询索引	实现了对医疗数据的访问控制，提高了用户的查询效率	数据存储、数据共享	管理问题，需要耗费大量的人力和物力资源
Su 等[67]	构建搜索智能合约（SSC）和验证智能合约（VSC）	提高了搜索精度，解决了数据共享过程中的隐私保护问题，减轻了数据用户的计算负担	数据检索、数据共享	安全性问题，易受到黑客攻击，执行效率问题，需要消耗大量的资源
Li 等[68]	上链分类账和下链存储（OLOS），基于格密码的安全关键字搜索	减轻了公共分类账的负担，节省了公共云空间，并具有抵抗量子攻击的能力	数据存储、数据共享、数据检索	计算复杂度高，密钥管理问题，实现难度大

3.3 基于区块链的可搜索属性加密隐私保护

基于区块链的可搜索属性加密技术是一种创新性的安全解决方案，旨在实现对加密数据的高效搜索和访问控制，同时保护数据的隐私和安全性。B-SABE 将数据加密，并通过属性加密技术实现对数据的访问控制，以确保数据的完整性和安全性。然而，目前 B-SABE 仍然存在一些问题，例如可扩展性差。在实际应用中，B-SABE 需要存储大量的索引和密文数据，导致存储和计算资源不足、数据隐私和安全性共享面临威胁等问题。在 B-SABE 技术中，访问控制是基于属性实现的，但当用户的属性发生变化时，需要撤销其相应的访问权限。此外，还需要解决可验证可审计的问题，以确保系统的透明性和可信度。本小节将从多关键字搜索、动态权限可撤销

以及完整性验证3个方面对基于区块链的可搜索属性加密技术应用进行概括综述。

3.3.1 多关键字搜索方案

多关键字搜索方案允许用户输入多个关键字进行检索并返回与之相关的结果。随着传统医疗记录的数字化,医疗机构面临着电子病历隐私泄露等问题。患者和医生在访问电子健康记录时花费大量时间查询所需数据,但所获得的数据不一定正确。Niu等[69]利用多项式方程实现关键字的任意连接,检索效率较高。Guo等[66]提出了基于属性加密的跨域搜索方案,关键字搜索形式实现了灵活的密文搜索。Li等[70]提出了一种基于格密码的安全关键字搜索属性加密(KS-ABE)方案。Feng等[71]将分层属性加密与线性秘密共享相结合,提出了一种基于可搜索属性加密的区块链数据隐私保护方案,避免了区块链网络私钥和访问结构泄露的安全风险;将私钥组件与用户节点随机关联,解决了合谋攻击问题。为了进一步提高检索效率,降低吞吐量和延迟,Hussien等[72]提出了一种基于智能合约的属性可搜索加密(SC-ABSE)访问控制方案,通过基于密文策略属性加密和可搜索对称加密,以及决策双线性迪菲-赫尔曼硬度假设(DB-DH)和离散对数(dL)问题,实现了多关键字搜索。快速高效的关键字搜索是实现这一目标的关键第一步,Su等[73]基于以太坊构建了两个智能合约,即搜索智能合约(SSC)和验证智能合约(VSC),实现了一种只返回top-k的排序多关键字搜索方案,保证了共享数据的保密性和访问权限,以及隐藏策略机制。区块链存在一种"验证者困境"现象,缺乏可靠验证,现有可搜索加密方案所使用的top-k查询技术在检索过程中不能根据用户需求对搜索结果进行过滤,导致生成了大量无效的访问列表。Yan等[74]提出了一种基于区块链的多关键字排序可搜索方案,数据所有者(DO)可以撤销授权数据用户(DU)搜索权限,利用单调加权函数聚合,提高了检索的效率。传统基于云服务器的关键字搜索,中心权限过大,容易造成中心单点故障。Wu等[75]提出了一种基于联盟区块链和基于属性加密的多权限、多云关键字搜索方案,通过在活门匹配过程中隐藏关键字和访问策略来实现隐私保护。表7列举了相关工作的多关键字搜索性能的比较。

表7 多关键字搜索性能比较

Table 7 Comparison of multi-keyword search performance

相关工作	索引生成阶段	搜索阶段	搜索令牌生成阶段	访问策略	特点
Niu等[69]	$(2V+M+2)P$	$(V+M+2)E$	$(N+1)$P	Tree	利用多项式方程实现关键字的任意连接
Guo等[66]	$N(V+2M+3)\log q$	$n(N+1)\log q$	$n(N'+1)\log q$	Lsss	支持跨域搜索的数据共享方案
Feng等[71]	$H+3P+E$	$H+P$	$2P+P$	And	分层属性加密与线性秘密共享相结合
Hussien等[72]	$P(V+1)$	$SKE+P(2M+1)HM$	$3P+1$	And	基于决策双线性迪菲-赫尔曼硬度假设(DB-DH)和离散对数(dL)问题,实现了多关键字搜索
Su等[73]	$(4V+2)E+E_1$	$3E$	E_1+2P'	And	top-k的排序多关键字搜索
Yan等[74]	$2P+2H$	$P+3E$	$(2N+1)P+N(T+H)$	And	利用单调加权函数聚合,提高检索的效率
Wu等[75]	$(2N+4)P$	$2P'$	$4P+2T$	Lsss	通过在活门匹配过程中隐藏关键字和访问策略来实现隐私保护

注:P:指数运算;P':配对操作;E,E_1:双线性运算;N:搜索关键字个数;N':陷门关键字个数;M:所有关键字个数;n:格的参数;V:属性个数;q:安全系数;H:哈希操作;SKE:对称密钥算法;T:乘法运算。

3.3.2 动态权限可撤销方案

本小节对基于区块链的可搜索属性加密方案中的动态权限可撤销方案进行了分析和总结。

传统的加密和搜索原语,包括基于属性加密和带有关键字搜索的公钥加密。Pournaghi等[37]提出了一种基于区块链和基于属性加密的医疗数据记录和存储方案MedSBA,该方案采用私有区块链,在MedSBA中用于改善撤销即时访问。Lu等[76]提出了一种可搜索属性加密系统,用联盟区块链代替传统的密钥生成中心来生成和管理密钥,用户只需要花费很少的计算成本就可以实现加解密操作。然而在解密和撤销方面存在较高的开销,并且在搜索中存在隐私泄露问题。Liu等[77]提出了一种具有高效撤销和解密的区块链辅助可搜索属性加密(BC-SABE)方案,区块链负责密钥的管理和用户权限的撤销。此外,Yu等[78]提出了一种高效可撤销和可搜索的多权限ABE(MA-ABE)方案ERS-ABE,区块链实现基于关键字的搜索和动态用户的管理,智能合约用于用户权限的动态撤销。Ambike等[79]提出了一种具有高效撤销和解密功能的区块链辅助可搜索属性加密算法(BC-SABE),将传统的集中式服务器替换成分布式区块链系统,由区块链进行参数的生成,以及密钥管理和用户撤销。为了保证多个数据用户能够访问数据,实现用户权限的动态变化,Song等[80]提出了一种基于区块链密文可更新可搜索加密方案,当数据用户需要更改访问策略或撤销某些用户的访问权限时,可以利用代理重加密技术实现数据请求者的属性撤销和密文更新。在此基础上,Niu等[81]利用验证算法保证云上数据的完整性,采用代理重加密技术实现用户的属性撤销。云辅助MIoT在开放医疗场景中的实际部署引发了对数据安全和用户隐私的担忧,为此,Bao等[82]提出了一种高效、可撤销、保护隐私的细粒度数据共享关键字搜索(ERPF-DS-KS)方案,基于伪身份的签名机制来保证数据的真实性。

3.3.3 完整性验证方案

数据完整性验证是指对数据进行检查和验证,以确保其在存储、传输或处理过程中没有发生未经授权的修改、损坏或篡改。本小节对基于区块链的可搜索属性加密方案的数据完整性验证进行了分析和总结。

针对隐私泄露、关键字搜索能力有限以及个人在搜索过程中控制权丧失的问题,Wan等[83]提出了一个基于区块链的数据完整性验证健康记录共享方案,采用可搜索的对称加密和基于属性加密来实现隐私保护。在此基础上,为了解决数据交换、互操作性差等问题,Zhang等[84]提出了一种基于区

块链的可搜索可验证加密 EMR 数据共享方案，提出了一个混合链，包括财团链和私人链，实现了电子病历的安全存储和共享。此外，针对多对多搜索模式下医院电子病历检索中共享用户身份授权的不便和缺乏正确性验证的问题，Niu 等[85]提出了一种支持验证的区块链辅助可搜索属性加密方案。针对医疗物联网患者无法掌握其医疗记录的问题，Yang 等[86]提出了一种患者控制的、云链协同的基于多权限属性电子病历共享加密方案，该加密具有可验证的外包解密和隐藏访问策略，利用 Shamir 秘密共享和智能合约在多个权威机构之间建立信任。区块链访问控制方案多为单向访问控制，不能满足密文搜索、数据双向确认、数据安全传输等需求。因此，Xu 等[87]提出了一种基于区块链辅助的可搜索加密双向属性访问控制方案(STW-ABE)，双向访问控制满足了用户与数据之间的相互确认。针对一对多搜索模型下共享解密密钥缺乏细粒度访问控制且搜索结果缺乏正确性验证的问题，Yan 等[88]提出了一种基于区块链且支持验证的属性搜索加密方案。该方案通过对共享密钥采用密文策略属性加密机制，实现了细粒度访问控制，解决了半诚实且好奇的云服务器模型下返回搜索结果不正确的问题，减少了用户计算开销，满足了自适应选择关键词语义安全，很好地保护了用户的隐私以及数据的安全。

3.4 方案对比

属性加密侧重于访问控制，ABE 允许将访问控制策略与加密数据相关联。其使用属性来定义访问规则，只有满足这些属性条件的用户才能解密和访问数据。这种技术在保护数据隐私和确保数据安全的同时，提供了细粒度的访问控制能力。

可搜索加密侧重于在保护数据的前提下实现搜索功能，可搜索加密允许对加密数据进行搜索，而无需将其解密。这种技术可以在保护用户隐私的同时，使得数据在加密状态下仍然可以进行高效的查询操作。

区块链技术侧重于去中心化和可追溯性。区块链是一种分布式账本技术，通过将交易数据记录在区块中，并使用加密技术来保护数据的完整性。区块链的设计目标是实现去中心化、不可篡改和可追溯的交易记录。它通常用于建立信任和可靠性，例如在加密货币和供应链管理等领域。

尽管这些技术在某些方面有不同，但是根据具体的应用场景和需求，可以将这 3 种技术进行有机的结合，来满足相应的隐私安全要求。

例如要实现隐私保护，属性加密和可搜索加密都具有保护数据隐私的能力。通过将属性加密和可搜索加密与区块链结合，可以在分布式的区块链网络中实现数据的隐私保护，只有满足特定属性条件的节点才能解密和搜索数据，同时，区块链技术可以确保数据的完整性和不可篡改性。其次，如果希望不依赖于第三方机构，属性加密和可搜索加密可以通过区块链实现去中心化的访问控制和搜索。区块链提供了一个共享的分布式账本，其中包含属性条件、搜索索引和访问控制策略。这样就不再依赖单一的中心化机构来控制访问和搜索操作，而是由区块链网络中的参与者共同管理和验证。区块链技术的特性可以为属性加密和可搜索加密提供可追溯性。通过将访问控制和搜索操作的记录写入区块链中，可以实现对数据访问和使用的审计追溯，这种整合可以增加数据使用的透明度和可信度，确保数据使用符合规定和政策。可搜索加密通常需要建立索引以支持高效的搜索操作，通过将索引存储在区块链上，可以实现去中心化的索引管理，为数据检索提供了安全性和可扩展性。

基于区块链的可搜索属性加密是将属性加密、可搜索加密和区块链进行整合的一种应用方式，它结合了属性加密的访问控制能力、可搜索加密的高效搜索功能和区块链的去中心化、可追溯性等特性。这种结合可以应用于如分布式存储、医疗保健记录、供应链管理等需要同时保护隐私并且实现可搜索功能的场景中。

表 8 对比了基于区块链的可搜索属性加密技术、基于区块链的属性加密技术以及基于区块链的可搜索加密技术各自的特点、优缺点以及搜索灵活性和面临的问题与挑战。

表 8 基于区块链的可搜索属性加密技术对比

Table 8 Comparison of searchable attribute encryption technologies based on blockchain

方案	方法	优点	计算复杂度	存储占用	通信开销	存在问题
基于区块链的可搜索加密	允许用户在加密数据上执行搜索操作，而无需解密数据	加密数据	中等，涉及搜索操作	中等，需要存储索引结构	中等，需要传输额外的索引数据	可搜索加密技术的搜索效率较明文搜索低
基于区块链的属性加密	是一种将访问策略与密文绑定的加密方法	灵活的访问控制	高，涉及复杂的数学运算	低，不需要明文存储数据	低，不需要频繁传输大量数据	访问策略过于复杂，导致属性管理困难
基于区块链的可搜索属性加密	结合可搜索加密和属性加密优点，保证访问控制同时实现了加密数据高效检索	使数据访问更灵活支持加密数据搜索	高，涉及访问控制及加解密运算	高，需要存储属性信息和索引	高，需要传输属性信息和索引	结合可搜索加密和属性加密的计算开销可能导致性能下降 提高搜索效率和灵活性可能降低系统安全性

4 问题与挑战

本文综述了将区块链和可搜索属性加密技术结合来提高数据安全和用户隐私保护的方案。分别从多关键字搜索、多权限动态撤销访问控制、访问策略隐藏这 3 个方面进行了分析，区块链结合属性可搜索加技术可以在一定程度提高数据的检索效率，保证数据隐私共享安全。由于存在大规模数据集的情况，不断的加密解密会导致通信计算开销增大，其次，单关键字搜索将无法满足实时更新的数据检索。当用户退出节点后，附属的访问权、密文密钥需动态实时更新，若采用单个权限管理，将会很大程度上降低区块链的可扩展性。访问策略是控制数据访问的重要信息，它包含了哪些用户可以访问哪些数据以及访问时需要满足的条件等信息，如果访问策略泄露，攻击者可能会利用该信息来获取用户隐私数据并发起攻击。所以未来基于区块链的可搜索属性加密技术应用研究的方向有以下 3 个方面。

1)多权限动态可撤销访问控制

基于区块链的多权限动态可撤销访问控制主要利用区块链的去中心化、不可篡改和可追溯性特点,实现访问控制的动态管理。传统的访问控制机制通常只能基于用户身份或角色来控制访问权限,权限过于单一,易遭受单点攻击,而且难以解决权限的动态实时更新问题。随着用户属性及数据集规模的增大,研究应更加注重细粒度的访问控制,如基于智能合约的自动访问控制管理、引入 Shamir 秘密共享方案,实现每个属性由多个权限联合管理,以避免单点故障,或者基于代理重加密的密钥管理等。在实现动态访问控制的同时,可以保证数据所有者灵活更新访问控制策略,达到可撤销可搜索的功能,实现对数据隐私的安全保护。未来多权限访问如何应对复杂的应用场景设置合理的访问控制策略,以及随着数据集的增大,访问控制策略如何快速地扩展以满足新的需求,是需要研究的一个问题。

2)属性访问策略隐藏

访问控制策略通常包含一些敏感信息,如用户的个人信息、角色、权限等。属性访问策略隐藏主要用于保护策略本身,防止策略信息泄露。在传统的访问控制机制中,访问控制策略通常是硬编码在应用程序中的,这使得对访问控制策略进行修改和扩展变得非常困难。其次,访问控制机制需要对每个用户的权限进行维护,随着系统规模的增加,管理和维护也变得越来越困难。属性访问策略的隐藏是将访问控制策略与应用程序解耦,从而提高其灵活性和可扩展性。例如,基于双线性配对的属性基加密(ABE)算法采用参数优化的加性同态 Paillier 密码体制保护患者隐私,以及基于部分密文的半策略隐藏和动态权限更改功能等,目的在于可以解决大范围属性系统中用户属性隐私和策略隐私泄漏的问题。随着访问控制策略的复杂性不断增加,有效地管理和维护访问策略成为一个重要的问题,一些研究意在采用智能合约的方式实现开发自动化的策略管理技术,以提高系统的效率。同时由于用户属性是一个动态变化的过程,如何动态地管理和分配用户属性也是一个有待优化和解决的问题。

3) 多关键字搜索

多关键字搜索主要解决在加密数据上进行高效、安全的关键字搜索问题。传统的关键字搜索往往只能根据关键字进行简单的匹配,难以有效地理解用户的查询意图,以及处理多个关键字的查询,因此,可以尝试将语义信息引入到关键字搜索中,以提高搜索的准确性。随着数据规模的不断增大,高效地实现大规模数据的多关键搜索成为了一个重要的研究方向。其次,随着数据共享的快速发展,个人隐私保护意识的不断增强,隐私数据易遭到泄露的情况下,如何在保护用户隐私的前提下实现可靠的关键字搜索也成为了目前一个热门的研究领域。近几年随着信息交叉与融合的深入发展,多模态跨领域多关键字搜索成为可能,但是目前不同模态的数据可能存在语义上的差异,以及多模态检索需要融合不同领域的知识,如何在保证跨模态正确理解语义的情况下实现高效的数据检索仍然是一个困难的问题。

基于区块链的属性加密可以实现更加精细的访问控制,使得只有满足特定属性的用户才能解密数据。这种技术在需要高度个性化的数据访问控制的领域有很大的应用潜力,如电子健康记录、云存储服务、物联网等。基于区块链的可搜索加密允许在加密数据上进行搜索,这在许多场景下都非常有用,如云存储、电子邮件服务、即时通讯等。基于区块链的可搜索属性加密结合了属性加密和可搜索加密的优点,允许在满足特定属性的加密数据上进行搜索。这种技术在需要同时实现精细的访问控制和数据搜索的场景下有很大的应用潜力,如企业数据管理、云计算、大数据分析等。

总的来说,这些技术都有助于实现数据的安全共享和利用,同时保护用户的隐私。但也需要注意,这些技术的实际应用还面临许多挑战。

结束语 本文主要对基于区块链的可搜索属性加密技术应用进行了综合性的研究和分析,全面梳理了该领域的研究现状,并从基于区块链的可搜索加密技术、基于区块链的属性加密技术以及基于区块链的可搜索属性加密技术 3 个应用方面进行了详细的介绍。希望为后续的研究提供一些有价值的参考。

在基于区块链的可搜索加密技术和基于区块链的属性加密技术方面,本文从多关键字搜索、属性访问策略隐藏、动态可撤销权限、审计完整性验证以及结合其他加密技术这 5 个方面进行了技术比较,并对其优缺点进行了深入剖析。比如,多关键字搜索可以提高查询效率,但可能降低数据安全性;属性访问策略隐藏有助于保护用户隐私,但实现起来较为复杂;动态可撤销权限有利于实现用户权限的动态管理,但需要解决权限撤销后如何保证数据安全的问题;审计完整性验证有助于确保数据的完全性,但可能引入额外的计算开销。

在基于区块链的可搜索属性加密技术应用方面,本文集中分析了这一技术如何将可搜索加密技术和属性加密技术相结合,实现数据的安全存储和高效查询。文章提出了这一技术在多关键字搜索、属性访问策略隐藏、动态可撤销权限、审计完整性验证以及结合其他加密技术等方面的应用优势,如提升查询效率、强化用户隐私保护、实现用户权限的动态管理、确保数据的安全性等。相较于基于区块链的可搜索加密技术和基于区块链的属性加密技术,基于区块链的可搜索属性加密技术具有更高的安全性和实用性。它充分利用了区块链技术的去中心化、不可篡改和可追溯等特性,实现了数据的安全存储和高效查询,同时还提供了细粒度的访问控制和动态权限管理,有力地保护了用户隐私。然而,基于区块链的可搜索属性加密技术应用仍然面临一些挑战,如计算复杂性高、存储开销大以及在大规模数据处理中的性能瓶颈等。总之,基于区块链的可搜索属性加密技术是一个非常值得研究的领域,可以为数据隐私和安全存储提供有效的解决方案。未来的研究可以着力于解决该技术面临的挑战和限制,提高算法效率,加强安全性和隐私保护,同时探索与其他技术的结合,以实现更加高效、安全、实用的数据存储和查询。

参 考 文 献

[1] WU Q,LI L J,MA X J. Review of research on attribute-based encryption supporting circuit structures[J]. Journal of Xi'an University of Posts and Telecommunications, 2020,25(4):1-7,18.

[2] HUANG Y C,LI S S,YU B. Review of symmetric searchable encryption in cloud environment[J]. Journal of Electronics and Information,2023,45(3):1134-1146.

[3] NIU S F,CHEN L X,WANG J F,et al. lectronic Health Record

Sharing Scheme With Searchable Attribute-Based Encryption on Blockchain[J]. IEEE Access, 2020, 8: 7195-7204.

[4] XUE L Q. The Application of Blockchain Technology in the Financial Field[C]// 2021 International Conference on Forthcoming Networks and Sustainability in AIoT Era (FoNeS-AIoT). 2021: 130-134.

[5] AL-DAHHAN R, SHI Q, LEE G M. et al. Survey on Revocation in Ciphertext-Policy Attribute-Based Encryption [J]. Sensors Basel, Switzerland, 2019, 19(7): 1695.

[6] WANG S Y, WANG J M, DONG Q F, et al. Review of attribute-based encryption technology[J]. Journal of Information Network Security, 2019, 225(9): 76-80.

[7] CHAUDHARI N, SAINI M, KUMAR A. A Review on Attribute Based Encryption[C]// Proceedings of the 2016 8th International Conference on Computational Intelligence and Communication Networks. Nainital: CICN. 2016: 380-385.

[8] HOW H, HENG S. Blockchain-Enabled Searchable Encryption in Clouds: A Review[J]. J. Inf. Secur., 2022, 67: 103183.

[9] VARRI U, PASUPULETI S, KADAMBARI, et al. A scoping review of searchable encryption schemes in cloud computing: taxonomy, methods, andrecent developments[J]. Journal of Supercomputing, 2019(76): 3013-3042.

[10] XIE Q Q, YANG N M, FENG X. Review of blockchain transaction privacy protection technology[J]. Journal of Computer Application, 2023, 43(10): 2996-3007.

[11] DU R, MA C, LI M. Privacy-Preserving Searchable Encryption Scheme Based on Public and Private Blockchains[J]. Tsinghua Science and Technology, 2022, 28(1): 13-26.

[12] MAMTA, BRIJ B G, LI K C, et al. Blockchain-Assisted Secure Fine-Grained Searchable Encryption for a Cloud-Based Healthcare Cyber-Physical System[J]. IEEE/CAA Journal of Automatica Sinica, 2021, 8(21): 1877-1890.

[13] NIU J, LI X, GAO J, et al. Blockchain-Based Anti-Key-Leakage Key Aggregation Searchable Encryption for IoT[J]. IEEE Internet of Things Journal, 2020(7): 1502-1518.

[14] GAO H M, LUO S S, MA Z F, et al. BFR-SE: A Blockchain-Based Fair and Reliable Searchable Encryption Scheme for IoT with Fine-Grained Access Control in Cloud Environment[J]. Wireless Communications and Mobile Computing, 2021, 2021: 5340116.

[15] XU C, YU L, ZHU L, et al. A blockchain-based dynamic searchable symmetric encryption scheme under multiple clouds[J]. Peer-to-Peer Netw., 2021, 14: 3647-3659.

[16] ZHANG C, FU S J, AO W J, et al. A Blockchain Based Searchable Encryption Scheme for Multiple Cloud Storage[C]// Proceedings of International Conference on Cryptography and Security Systems. UK: CSS. 2019.

[17] YANG X D, LI X X, CHEN A J, et al. Blockchain-based Searchable Proxy Re-encryption Scheme for EHR Security Storage and Sharing[C]// Proceedings of Journal of Physics: Conference Series. IOP: JPCS, 2021(828).

[18] CHEN B W, WU L B, WANG H Q, et al. A Blockchain-Based Searchable Public-Key Encryption With Forward and Backward Privacy for Cloud-Assisted Vehicular Social Networks[J]. IEEE Transactions on Vehicular Technology, 2020(69): 5813-5825.

[19] XU G, XU S Y, CAO Y B, et al. PPSEB: A Postquantum Public-Key Searchable Encryption Scheme on Blockchain for E-Healthcare Scenarios [J]. Security and Communication Networks, 2022, 2022: 3368819.

[20] YANG Y Y, HU M S, CHENG Y G, et al. Keyword Searchable Encryption Scheme based on Blockchain in Cloud Environment [C]// Proceedings of the 2020 3rd International Conference on Smart BlockChain. Tokyo: Smart Block, 2020.

[21] YAN X X, YUAN X H, YE Q, et al. Blockchain-Based Searchable Encryption Scheme With Fair Payment[J]. IEEE Access, 2020(8): 109687-109706.

[22] YANG C J, XIE D D, CAI LX, et al. FBPB-SE: A Forward and Backward Private Blockchain-based Searchable Encryption with Fuzzy Multi-keyword[C]// DASC. 2022.

[23] XU W S, ZHANG J B, YUAN Y L, et al. Towards efficient verifiable multi-keyword search over encrypted data based on blockchain[J]. PeerJ Computer Science, 2022(8): e930.

[24] XU C, ZHANG P, MEI L, et al. Ranked searchable encryption based on differential privacy and blockchain[J/OL]. http://api.semanticscholar.org/CorpusID:252134312.

[25] AITIZAZ A, ALMAIAH M A, HAJJEJ F, et al. An Industrial IoT-Based Blockchain-Enabled Secure Searchable Encryption Approach for Healthcare Systems Using Neural Network[J]. Sensors (Basel, Switzerland), 2022, 22(2): 572.

[26] LI H Y, WANG T, QIAO Z R, et al. Blockchain-based searchable encryption with efficient result verification and fair payment[J]. J. Inf. Secur. Appl., 2021(58): 102791.

[27] WANG T, WANG J Y, YANG Q L, et al. An Efficient Verifiable Searchable Enc. ryption Scheme With Aggregating Authorization for Blockchain-Enabled IoT[J]. IEEE Internet of Things Journal, 2022, (20): 20666-20680.

[28] DU R, WANG Y. Verifiable Blockchain-Based Searchable Encryption with forward and backward privacy[C]// Proceedings of the 2020 16th International Conference on Mobility, Sensing and Networking (MSN). NJ: IEEE, 2020.

[29] GUO Y, ZHANG C, JIA X. Verifiable and Forward-secure Encrypted Search Using Blockchain Techniques[C]// 2020 IEEE International Conference on Communications (ICC 2020). Dublin, Ireland: IEEE, 2020.

[30] DU H, CHEN J, LIN F, et al. A Lightweight Blockchain-based Public-Key Authenticated Encryption with Multi-Keyword Search for Cloud Computing[J]. Security and Communication Networks, 2022, 2022: 2309834.

[31] LI Z H, MA Z F. A blockchain-based credible and secure education experience data management scheme supporting for searchable encryption[J]. China Communications, 2021(18): 172-183.

[32] YANG X, LI T, LIU R, et al. Blockchain-Based Secure and Searchable EHR Sharing Scheme[C]// Proceedings of the 2019 4th International Conference on Mechanical, Control and Computer Engineering. Hohhot: ICMCCE, 2019.

[33] ZHANG Y, WEN L, ZHANG Y, et al. Deniably authenticated searchable encryption scheme based on Blockchain for medical image data sharing[J]. Multimedia Tools and Applications, 2020(79): 27075-27090.

[34] QIN X M, HUANG Y F, YANG Z, et al. A Blockchain-based access control scheme with multiple attribute authorities for se-

cure cloud data sharing[J]. Journal of Systems Aarchitecture, 2021,112(1):101854.

[35] LIU C L,XIANG F,SUN Z X. Multiauthority Attribute-Based Access Control for Supply Chain Information Sharing in Blockchain[J]. Security and Communication Networks,2022,2022:8497628.

[36] GUO L,YANG X,YAU W C,et al. TABE-DAC:Efficient Traceable Attribute-Based Encryption Scheme With Dynamic Access Control Based on Blockchain[J]. IEEE Access,2021(9):8479-8490.

[37] POURNAGHI S M,BAYAT M,FARJAMI Y,et al. MedSBA:a novel and secure scheme to share medical data based on blockchain technology and attribute-based encryption[J]. Journal of Ambient Intelligence and Humanized Computing, 2020, 11:4613-4641.

[38] SHARMA P,JINDAL R,BORAH,et al. Blockchain-based cloud storage system with CP-ABE-based access control and revocation process[J]. J Supercomput,2022,78:7700-7728.

[39] YU J G,LIU S H,XU M H,et al. An Efficient Revocable and Searchable MA-ABE Scheme With Blockchain Assistance for C-IoT[J]. IEEE Internet of Things Journal,2023(10):2754-2766.

[40] XIAO M,HUANG Q,MIAO Y,et al. Blockchain Based Multi-Authority Fine-Grained Access Control System With Flexible Revocation[C]// 2022 IEEE World Congress on Services(SERVICES). Barcelona,Spain,2022:31-31.

[41] GAO H M,MA Z F,LUO S S,et al. BSSPD:A Blockchain-Based Security Sharing Scheme for Personal Data with Fine-Grained Access Control[J]. Wireless Communications and Mobile Computing,2021,2021:20.

[42] YANG X,ZHANG C. Blockchain-Based Multiple Authorities Attribute-Based Encryption for EHR Access Control Scheme [J]. Applied Sciences,2022,12(21):10812.

[43] ALSHEHRI M,PANDA B,ALMAKDI S,et al. A Novel Blockchain-Based Encryption Model to Protect Fog Nodes from Behaviors of Malicious Nodes[J]. Electronics,2021,10(24):3135.

[44] GUO R,SHI H,ZHENG D,et al. Flexible and Efficient Blockchain-Based ABE Scheme With Multi-Authority for Medical on Demand in Telemedicine System[C]// IEEE Access, 2019:88012-88025.

[45] GUO R,SHI H,ZHAO Q,et al. Secure Attribute-Based Signature Scheme With Multiple Authorities for Blockchain in Electronic Health Records Systems[C]// IEEE Access. 2018:11676-11686.

[46] LI X,CHEN Y,ZHU H,et al. An Access Control Scheme Supporting Privacy Protection Based on Blockchain and Attribute [C]// Proceedings of the Journal of Physics:Conference Series. IOP:JPCS,2021.

[47] YANG X,CHEN A,WANG Z,et al. Cloud Storage Data Access Control Scheme Based on Blockchain and Attribute-Based Encryption[J]. Security and Communication Networks, 2022, 2022:2204832.

[48] YANG M,LIU N,WANG D,et al. Grid data sharingscheme based on blockchain and hybrid encryption[C]// Proceedings of the the Conference on Mechatronics and Computer Technology Engineering. IOP:EI,2022.

[49] QIN C,WU L,MENG W,et al. A privacy-preserving blockchain-based tracing model for virus-infected people in cloud[J]. Expert Systems with Applications,2022(211):118545-118545.

[50] ZHANG Y,WEI X,CAO J,et al. Blockchain-Enabled decentralized Attribute-Based access control with policy hiding for smart healthcare[J]. J. King Saud Univ. Comput. Inf. Sci,2022(34):8350-8361.

[51] LI F,LIU K,ZHANG L,et al. EHRChain:A Blockchain-Based EHR System Using Attribute-Based and Homomorphic Cryptosystem[J]. IEEE Transactions on Services Computing,2021,15:2755-2765.

[52] MITTAL S,GHOSH M. A novel two-level secure access control approach for blockchain platform in healthcare[J]. International Journal of Information Security,2023,22:799-817.

[53] WANG H,SONG Y. Secure Cloud-Based EHR System Using Attribute-Based Cryptosystem and Blockchain[J]. Journal of Medical Systems,2018(42):1-9.

[54] XU G X,ZHANG J J,UCHANI G O C,et al. An efficient blockchain-based privacy-preserving scheme with attribute and homomorphic encryption[J]. International Journal of Intelligent Systems,2022,37(12):10715-10750.

[55] LIANG W,YANG Y,YANG C,et al. PDPChain:A Consortium Blockchain-Based Privacy Protection Scheme for Personal Data [J]. IEEE Transactions on Reliability,2022,72(2):586-598.

[56] ZHANG G F,CHEN X,ZHANG L,et al. STAIBT:Blockchain and CP-ABE Empowered Secure and Trusted Agricultural IoT Blockchain Terminal[J]. Int. J. Interact. Multim. Artif. Intell.,2022,7(5):66-75.

[57] BAEKS,정보보호학과, 고.정. Blockchain-based Electronic Medical Record Sharing Framework Using Ciphertext Policy Attribute-Based Cryptography for patient's anonymity[J]. Jouranl of Information and Security,2019(3):49-60.

[58] ULLAH Z,RAZA B,SHAH H,et al. Towards Blockchain-Based Secure Storage and Trusted Data Sharing Scheme for IoT Environment[J]. IEEE Access,2022(10):36978-36994.

[59] YUAN J,MA Y,LUO W. B-SSMD:A Fine-Grained Secure Sharing Scheme of Medical Data Based on Blockchain[J]. Security and Communication Networks,2022,2022:2719951.

[60] HE Y,WANG H Y,LI Y,et al. An Efficient Ciphertext-Policy Attribute-Based Encryption Scheme Supporting Collaborative Decryption With Blockchain[J]. IEEE Internet of Things Journal,2022,9(4):2722-2733.

[61] ZHANG L,PENG M,WANG W,et al. Secure and Efficient Data Storage and Sharing Scheme Based on Double Blockchain[J]. Computer,Materials & Continua,2021,66(1):499-515.

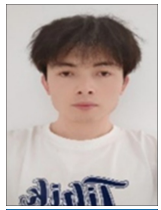
[62] CHEN J H,YIN X C,NING J T. A fine-grained and secure health data sharing scheme based on blockchain[J]. Transactions on Emerging Telecommunications Technologies, 2022, 33(9):e4510.

[63] TAO J,LING L. Practical Medical Files Sharing Scheme Based on Blockchain and Decentralized Attribute-Based Encryption [J]. IEEE Access,2021(9):118771-118781.

[64] LI X,DONG X M,XU X H,et al. A Blockchain-Based Scheme for Efficient Medical Data Sharing with Attribute-Based Hierarchical Encryption[C]// Proceedings of the Web Information System and Application Conference. NJ:IEEE,2022.

[65] NIU S,CHEN L,WANG J,et al. Electronic Health Record Sha-

ring Scheme With Searchable Attribute-Based Encryption on Blockchain[J]. IEEE Access, 2020(8): 7195-7204.
[66] GUO K, HAN Y, WU R, et al. CD-ABSE: Attribute-Based Searchable Encryption Scheme Supporting Cross-Domain Sharing on Blockchain[J]. Wireless Communications and Mobile Computing, 2022, 2022: 6719302.
[67] SU J, ZHANG L, MU Y. BA-RMKABSE: Blockchain-aided Ranked Multi-keyword Attribute-based Searchable Encryption with Hiding Policy for Smart Health System[J]. Future Gener. Comput. Syst., 2022(132): 299-309.
[68] LI C Y, DONG M X, LI J, et al. Efficient Medical Big Data Management With Keyword-Searchable Encryption in Healthchain. IEEE Systems Journal[J]. 2022(16): 5521-5532.
[69] NIU S, CHEN L, WANG J, et al. Electronic Health Record Sharing Scheme With Searchable Attribute-Based Encryption on Blockchain[J]. IEEE Access, 2020(8): 7195-7204.
[70] LI C, DONG M, LI J, et al. Efficient Medical Big Data Management With Keyword-Searchable Encryption in Healthchain[J]. IEEE Systems Journal, 2022(16): 5521-5532.
[71] FENG T, PEI H, MA R, et al. Blockchain Data Privacy Access Control Based on Searchable Attribute Encryption[J]. Computers, Materials, &Continua, 2020, 66(1): 871-884.
[72] MANSUR H H, RASIN S M, UDZIR N I, et al. Blockchain-Based Access Control Scheme for Secure Shared Personal Health Records over Decentralised Storage[J]. Sensors (Basel, Switzerland), 2021, 21(7): 2462.
[73] SU J, ZHANG L Y, MU Y. BA-RMKABSE: Blockchain-aided Ranked Multi-keyword Attribute-based Searchable Encryption with Hiding Policy for Smart Health System[J]. Future Gener. Comput. Syst., 2022, 132(C): 299-309.
[74] YAN X, FENG S, TANG Y, et al. Blockchain-based verifiable and dynamic multi-keyword ranked searchable encryption scheme in cloud computing[J]. J. Inf. Secur. Appl., 2022(71): 103353.
[75] WU Q, LAI T T, ZHANG L Y, et al. Blockchain-enabled multi-authorization and multi-cloud attribute-based keyword search over encrypted data in the cloud[J]. J. Syst. Archit., 2022(129): 102569.
[76] LU Z W, GUO Y Y, LI J, et al. Novel Searchable Attribute-Based Encryption for the Internet of Things[J]. Wireless Communications and Mobile Computing, 2022: 8350006.
[77] LIU S, YU J, XIAO Y, et al. BC-SABE: Blockchain-Aided Searchable Attribute-Based Encryption for Cloud-IoT[J]. IEEE Internet of Things Journal, 2020(7): 7851-7867.
[78] YU J, LIU S, XU M, et al. An Efficient Revocable and Searchable MA-ABE Scheme With Blockchain Assistance for C-IoT[J]. IEEE Internet of Things Journal, 2023(10): 2754-2766.
[79] AMBIKA N. Reliable Blockchain-Aided Searchable Attribute-Based Encryption for Cloud-IoT[J]. Advances in Systems Analysis, Software Engineering, and High Performance Computing, 2022, 2022: 238-250.
[80] SONG M, NIU S, FANG L. A ciphertext updatable attribute-based searchable encryption scheme via blockchain[C]// Proceedings of the 2021 2nd International Conference on Electronics, Communications and Information Technology. NJ: IEEE, 2021: 18-24.
[81] NIU S, CHEN L, LIU W. Attribute-Based Keyword Search Encryption Scheme with Verifiable Ciphertext via Blockchains[C]// Proceedings of the 2020 IEEE 9th Joint International Information Technology and Artificial Intelligence Conference. NJ: IEEE, 2020: 849-853.
[82] BAO Y, QIU W, TANG P, et al. Efficient, Revocable, and Privacy-Preserving Fine-Grained Data Sharing With Keyword Search for the Cloud-Assisted Medical IoT System[J]. IEEE Journal of Biomedical and Health Informatics, 2021(26): 2041-2051.
[83] WAN S, ZHANG D, ZHANG Y. Blockchain-Based Personal Health Records Sharing Scheme With Data Integrity Verifiable[J]. IEEE Access, 2019(7): 102887-102901.
[84] ZHANG Y, LIN S, ZHAO J. SV-DEMR: An Electronic Medical Record Data Sharing Scheme Based on Searchable and Verifiable Encryption via Consortium Blockchain[C]// ICBCTIS. 2022: 123-126.
[85] NIU S, SONG M, FANG L, et al. Keyword search over encrypted cloud data based on blockchain in smart medical applications[J]. Computer Commun., 2022, 192(C): 33-47.
[86] YANG X, ZHANG C. Blockchain-Based Multiple Authorities Attribute-Based Encryption for EHR Access Control Scheme[J]. Applied Sciences, 2022, 12(21): 10812.
[87] XU Z G, ZHANG S G, HAN H M, et al. Blockchain-Aided Searchable Encryption-Based Two-Way Attribute Access Control Research[J]. Security and Communication Networks, 2022, 2022: 2410455.
[88] YAN X X, YUAN X H, TANG Y L, et al. Attribute base search encryption scheme based on blockchain and supports validation[J]. Journal of Communication, 2020, 41(2): 187-198.



LAN Yajie, born in 1999, master candidate. His main research interest is the application of blockchain technology combined with attribute encryption in data privacy protection.

MA Ziqiang, born in 1990, Ph.D, associate professor. His main research interests include computer system security and blockchain application security.