边缘计算数据安全与隐私保护研究综述

张佳乐，赵彦超，陈兵，胡峰，朱琨
（南京航空航天大学计算机科学与技术学院，江苏 南京 211106）

摘 要：随着物联网、大数据和 5G 网络的快速发展和广泛应用，传统的云计算无法处理网络边缘设备所产生的海量数据，因此，边缘计算应运而生。然而，由于边缘计算的内容感知、实时计算、并行处理等开放特性，使在云计算环境下就已经存在的数据安全与隐私问题变得更加突出。阐述了边缘计算中数据安全与隐私保护的研究背景，提出以数据安全为中心的研究体系架构。围绕数据安全、访问控制、身份认证和隐私保护等关键技术，综述了近年来提出的可能适用于边缘计算数据安全与隐私保护的最新研究成果，并就方案的可扩展性和适用性进行分析讨论。此外，介绍了一些目前比较适用的边缘计算实例。最后，指出一些重要的研究方向和研究建议。

关键词：边缘计算；万物互联；数据安全；访问控制；身份认证；隐私保护
中图分类号：TP309
文献标识码：A
doi: 10.11959/j.issn.1000-436x.2018037

Survey on data security and privacy-preserving for the research of edge computing

ZHANG Jiale, ZHAO Yanchao, CHEN Bing, HU Feng, ZHU Kun
College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing 211106, China

Abstract: With the rapid development and extensive application of the Internet of things (IoT), big data and 5G network architecture, the massive data generated by the edge equipment of the network and the real-time service requirements are far beyond the capacity if the traditional cloud computing. To solve such dilemma, the edge computing which deploys the cloud services in the edge network has envisioned to be the dominant cloud service paradigm in the era of IoT. Meanwhile, the unique features of edge computing, such as content perception, real-time computing, parallel processing and etc., has also introduced new security problems especially the data security and privacy issues. Firstly, the background and challenges of data security and privacy-preserving in edge computing were described, and then the research architecture of data security and privacy-preserving was presented. Secondly, the key technologies of data security, access control, identity authentication and privacy-preserving were summarized. Thirdly, the recent research advancements on the data security and privacy issues that may be applied to edge computing were described in detail. Finally, some potential research points of edge computing data security and privacy-preserving were given, and the direction of future research work was pointed out.

Key words: edge computing, internet of everything, data security, access control, authentication, privacy-preserving

---

收稿日期：2017-09-28；**修回日期**：2018-02-07
通信作者：赵彦超，yczhao@nuaa.edu.cn
基金项目：国家自然科学基金资助项目（No.61672283, No.61602238）；国家重点研发计划基金资助项目（No.2017YFB0802303）；江苏省自然科学基金资助项目（No.BK20160805）
Foundation Items: The National Natural Science Foundation of China (No.61672283, No.61602238), The National Key Research and Development Program of China (No.2017YFB0802303), The Natural Science Foundation of Jiangsu Province (No.BK20160805)

1 引言

随着物联网技术和 5G 网络架构的快速发展，智能交通、智慧城市、位置服务、移动支付等新型服务模式和业务不断涌现。智能手机、可穿戴设备、联网电视以及其他传感设备数量将会呈现爆炸式增长趋势，随之而来的是物联网终端产生的“海量级”数据[1]。根据 2016 年思科云指数（GCI）的预测，到 2020 年，全球数据中心流量将达到 15.3 ZB[2]。同时，近几年的物联网设备连接数也呈现出线性增长趋势，据互联网业务解决方案集团（IBSG）预测，2020 年的物联网设备数量将达到 500 亿，如图 1 所示[3]。随后，“信息感知”的概念开始逐步延伸至物联网系统中，万物互联的边缘大数据处理时代[4,5]已经到来。相比于物联网而言，万物互联突破了传统物与物之间相互连接的限制，逐渐转变为以物联网感知层为代表的人与物之间的互联。其中，处于网络边缘的设备节点不再只是数据使用者的角色，而是正在向兼顾数据采集、模式识别、数据挖掘等大数据处理能力的计算节点转变。同时，这些边缘设备节点提供了丰富的服务接口，与云计算中心一起为用户提供协同式计算服务。

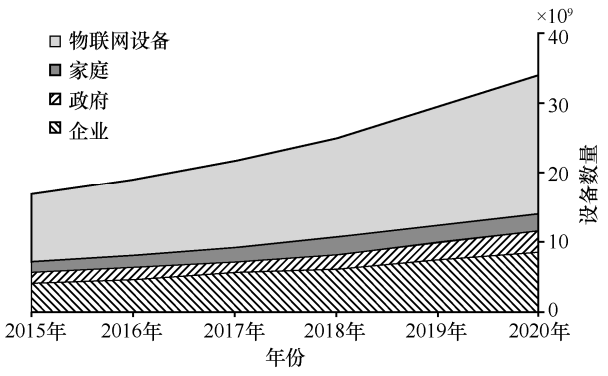


图 1 物联网设备增长趋势

传统的云计算模型无法满足万物互联的应用需求，其主要原因归纳起来主要有以下 4 个方面。

1) 多源异构数据处理。物联网的感知层数据处于海量级别，数据之间存在着频繁的冲突与合作，具有很强的冗余性、相关性、实时性和多源异构特性。融合的多源异构数据和实时处理要求给云计算带来了无法解决的巨大挑战。

2) 带宽负载和资源浪费。云服务是一种聚合度很高的集中式服务计算，用户将数据发送到云端存储和处理，将消耗大量的网络带宽和计算资源。同时，大量的用户访问也会增加网络流量，进而引发服务中断、网络时延等问题。

3) 资源受限。万物互联模式中的网络边缘设备通常是资源受限的（存储、计算能力和电池容量等），数据在边缘设备和云计算中心之间的长距离传输能耗问题显得尤为突出。

4) 安全和隐私保护。网络边缘数据涉及个人隐私，传统的云计算模式需要将这些隐私数据上传至云计算中心，这将增加泄露用户隐私数据的风险。

由于云计算模型与万物互联固有特征之间的矛盾，单纯依靠云计算这种集中式的计算处理方式，将不足以支持以物联网感知为背景的应用程序运行和海量数据处理，而且云计算模型已经无法有效解决云中心负载、传输宽带、数据隐私保护等问题。因此，边缘计算应运而生，与现有的云计算集中式处理模型相结合，能有效解决云中心和网络边缘的大数据处理问题[6,7]。边缘计算是指数据或任务能够在靠近数据源头的网络边缘侧进行计算和执行计算的一种新型服务模型。而这里所提的网络边缘侧可以是从数据源到云计算中心之间的任意功能实体，这些实体搭载着融合网络、计算、存储、应用核心能力的边缘计算平台，为终端用户提供实时、动态和智能的服务计算。同时，数据就近处理的理念也为数据安全和隐私保护提供了更好的结构化支撑。

随着边缘计算模型的深入研究，学术界和产业界相继提出了诸如移动云计算[8]（MCC）、雾计算[9]（FC）和移动边缘计算[10]（MEC）等新型边缘化计算模型。这些以网络边缘设备为核心的计算模式均为云计算任务向网络边缘迁移提供构架支撑，通过部署边缘服务设备（如雾节点、边缘服务器和私有云等），向移动终端提供多样化虚拟化服务，从而降低云计算中心的计算负载，减缓网络带宽压力，并能够在处理海量数据的同时确保高效的网络运营和服务交付，同时也改进了用户体验。尽管这些边缘计算模型的设计目标十分接近，但它们在实现这一目标的过程中会体现出一些根本性差异。一方面，MEC 平台的部署依赖于移动网络基础设施（如 5G），FC 中雾节点的部署点则可以是用户管理服务器、无线接入点、网关及路由等。而 MCC 的部署范围则更为广泛，在某些情况下甚至可以是移动终端来充当服务提供商。因此，在服务部署方面，目前只有电信运营商可以成为 MEC 服务提供

商，因为它拥有边缘数据中心部署所需的移动网络基础设施。相反，任何用户都可以部署自己的雾节点和 MCC 节点，甚至可以创建自己的私有云环境。另一方面，由于 MEC 和 FC 可以部署在运营商网络或 ISP 基础设施中，这使第三方服务提供商可以与运营商紧密合作，开发针对不同业务模式的定制服务，并提供这些服务的测试平台，为服务集成提供良好环境。这些边缘计算范式中的细小差别很有可能对边缘计算安全与隐私机制的构造产生不同程度的影响，因此，在开展相关研究工作时，应充分考虑方案的应用背景及固有特性，即适用性和可扩展性问题，这也是本文讨论已有研究工作的重点。

因此，由于边缘计算服务模式的复杂性、实时性，数据的多源异构性、感知性以及终端的资源受限特性，传统云计算环境下的数据安全和隐私保护机制不再适用于边缘设备产生的海量数据防护。数据的存储安全、共享安全、计算安全、传播和管控以及隐私保护等问题变得越来越突出。此外，边缘计算的另一个优势在于其突破了终端硬件的限制，使移动终端等便携式设备大量参与到服务计算中来，实现了移动数据存取、智能负载均衡和低管理成本。但这也极大地增加了接入设备的复杂度，由于移动终端的资源受限特性，其所能承载的数据存储计算能力和安全算法执行能力也有一定的局限性。边缘计算中的数据安全和隐私保护主要面临以下 4 点新挑战。

1) 边缘计算中基于多授权方的轻量级数据加密与细粒度数据共享新需求。由于边缘计算是一种融合了以授权实体为信任中心的多信任域共存的计算模式，使传统的数据加密和共享策略不再适用。因此，设计针对多授权中心的数据加密方法显得尤为重要，同时还应考虑算法的复杂性问题。

2) 分布式计算环境下的多源异构数据传播管控和安全管理问题。在边缘式大数据处理时代，网络边缘设备中信息产生量呈现爆炸性增长。用户或数据拥有者希望能够采用有效的信息传播管控和访问控制机制，来实现数据的分发、搜索、获取以及控制数据的授权范围。此外，由于数据的外包特性，其所有权和控制权相互分离，因此有效的审计验证方案能够保证数据的完整性。

3) 边缘计算的大规模互联服务与资源受限终端之间的安全挑战。由于边缘计算的多源数据融合特性、移动和互联网络的叠加性以及边缘终端的存储、计算和电池容量等方面的资源限制，使传统较为复杂的加密算法、访问控制措施、身份认证协议和隐私保护方法在边缘计算中无法适用。

4) 面向万物互联的多样化服务以及边缘计算模式对高效隐私保护的新要求。网络边缘设备产生的海量级数据均涉及个人隐私，使隐私安全问题显得尤为突出。除了需要设计有效的数据、位置和身份隐私保护方案之外，如何将传统的隐私保护方案与边缘计算环境中的边缘数据处理特性相结合，使其在多样化的服务环境中实现用户隐私保护是未来的研究趋势。

本文主要综述了边缘计算中数据安全和隐私保护的相关研究。介绍了边缘计算的基本概念、体系架构和面临的安全性问题，提出边缘计算中数据安全和隐私保护研究框架，并从数据安全、身份认证、访问控制和隐私保护这 4 个方面阐述了边缘计算的安全防护措施和最新的研究成果，最后给出了几点研究建议。

2　边缘计算数据安全与隐私保护研究体系

2.1　边缘计算架构与安全挑战

边缘计算中的“边缘”是个相对的概念，指从数据源到云计算中心数据路径之间的任意计算资源和网络资源。边缘计算允许终端设备将存储和计算任务迁移到网络边缘节点中，如基站（BS）、无线接入点（WAP）、边缘服务器等，既满足了终端设备的计算能力扩展需求，同时能够有效地节约计算任务在云服务器和终端设备之间的传输链路资源。边缘计算的体系架构如图 2 所示，主要包括核心基础设施、边缘数据中心、边缘网络和移动终端这 4 个功能层次。

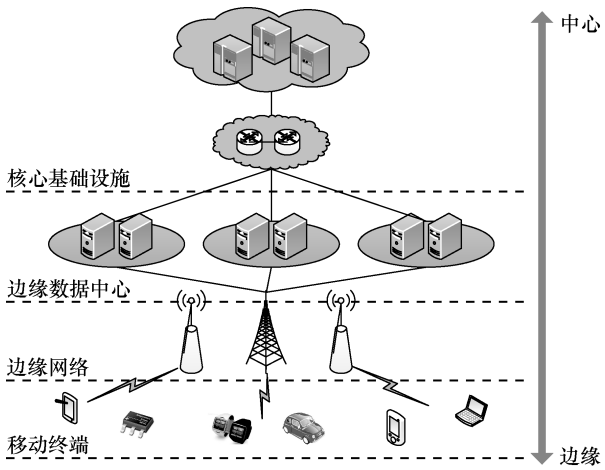


图 2　面向物联网的边缘计算体系架构

1) 核心基础设施为网络边缘设备提供核心网络接入以及集中式云计算服务和管理功能。其中，核心网络主要包括互联网络、移动核心网络、集中式云服务和数据中心等。而云计算核心服务通常包括 3 种服务模式：基础设施即服务（IaaS）、平台即服务（PaaS）和软件即服务（SaaS）。同时，在边缘计算服务模式下，允许多个云服务提供商同时为用户提供集中式的存储和计算服务。因此，可以通过部署多层次的异构服务器，来实现在各服务器之间的大规模计算迁移，而且能够为不同地理位置上的用户提供实时服务和移动代理。核心基础设施在很多情况下并不是完全可信的，因此，极有可能发生包括隐私泄露、数据篡改、拒绝服务攻击和服务操纵等威胁安全的攻击行为。

2) 边缘数据中心负责虚拟化服务和多个管理服务，是边缘计算中的核心组件之一，由基础设施提供商部署，搭载着多租户虚拟化基础设施。从第三方服务提供商到终端用户以及基础设施提供商自身都可以使用边缘数据中心提供的虚拟化服务。此外，网络边缘侧往往会部署多个边缘数据中心，这些数据中心在自主行动的同时又相互协作，但不会跟传统云端断开连接。因此，可以创建通过不同网络基础设施互联的分层体系架构，实现分布式协同计算服务模式。值得一提的是，边缘数据中心的数据安全性一直是终端用户十分关注的问题。边缘计算模式下的分布式并行数据处理方式使边缘计算平台存在数据保密性问题和隐私泄露现象。面临的安全挑战主要包括物理攻击、隐私泄露、服务操纵和数据篡改等。因此，研究边缘计算环境下的数据安全与隐私保护技术（如安全数据共享、访问控制、身份认证、隐私保护等）是保证边缘计算得以持续发展的重要支撑。

3) 边缘网络计算通过融合多种通信网络来实现物联网设备和传感器的互联，从无线网络到移动中心网络再到互联网络，在这种融合的网络构架中，其网络基础设施极易受到攻击，因为敌手可以对其中任何一个网络单元发起攻击。边缘网络中面临的主要安全威胁包括拒绝服务攻击、中间人攻击和伪造网关等。

4) 移动终端包括连接到边缘网络中的所有类型的设备（包括移动终端和众多物联网设备）。它们不仅是数据使用者的身份，而且还可以扮演数据提供者参与到各个层次的分布式基础设施中去。移动终端中的安全威胁主要有终端安全和隐私保护等，具体包括信息注入、隐私泄露、恶意代码攻击、服务操纵和通信安全等。

在以大数据为中心的边缘计算领域中，由于数据量的增加和实时性处理需求，集中式云中心数据处理将转变为云+边缘的双向计算模式。网络边缘设备不仅扮演着服务请求者的角色，而且还需要执行部分计算任务，包括数据存储、处理、搜索、管理和传输等。

2.2 数据安全与隐私保护研究体系

本文将边缘计算中数据安全与隐私保护研究体系划分为 4 个部分，分别是数据安全、身份认证、隐私保护和访问控制，如图 3 所示。

数据安全是创建安全边缘计算环境的基础，其根本目的在于保障数据的保密性和完整性。主要针对外包数据的所有权和控制权分离化、存储随机化等特性，用于解决数据丢失、数据泄露、非法数据操作等问题。同时，在此基础上允许用户进行安全数据操作。数据安全的主要内容包括数据保密性与

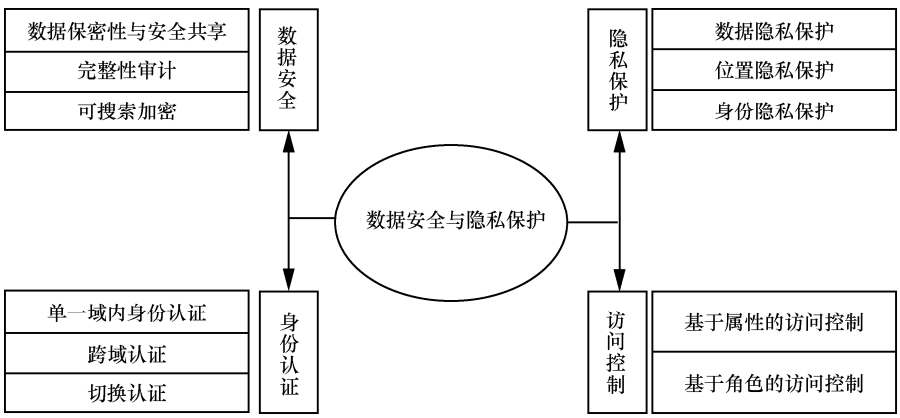


图 3 边缘计算数据安全与隐私保护研究体系

安全共享、完整性审计和可搜索加密。

物联网用户要想使用边缘计算所提供的计算服务，首先要进行身份认证。由于边缘计算是一种多信任域共存的分布式交互计算环境，因此，不仅需要为每一个实体分配身份，还需要考虑到不同信任域之间的相互认证。身份认证的主要研究内容包括单一域内身份认证、跨域认证和切换认证。

边缘计算中的授权实体并不都是可信的，而用户的身份信息、位置信息和私密数据都存储在这些半可信实体中，极易引发隐私问题。因此，在以开放式互联为背景的边缘计算中，隐私保护是一个备受关注的研究体系。其主要内容包括数据隐私保护、位置隐私保护和身份隐私保护。

访问控制是确保系统安全性和保护用户隐私的关键技术和方法，当前比较热门的访问控制方案包括基于属性和基于角色的访问控制，其中，基于属性的访问控制能够很好地适用于分布式架构，并实现细粒度的数据共享。

本文重点讨论数据安全防护技术、身份认证协议、访问控制系统和隐私保护等关键技术。重点介绍了基于密码技术的数据安全与隐私保护研究进展，并对一些可能的研究方向进行了展望。目前对边缘计算安全和隐私保护的研究工作尚处于初级阶段，已有的研究成果极少。其中，一个确实可行的研究思路是将现有的其他相关领域的安全技术移植到边缘计算环境中。国内外学者对移动云计算及其安全性展开了深入研究，Roman 等[11]对目前几种常见的移动边缘范式进行了安全性分析，阐述了一种通用协作的安全防护体系，并给出了研究意见，这些工作为边缘计算的安全性研究提供了理论参考。

3　数据安全

无论是云计算还是边缘计算，终端用户的私密性数据均需要部分或全部外包给第三方（如云计算数据中心和边缘数据中心），这就造成了存储在第三方数据中心的用户数据呈现出所有权和控制权分离化、存储随机化等特点，极易造成数据丢失、数据泄露、非法数据操作（复制、发布、传播）等数据安全性问题，数据的保密性和完整性无法得到保证。因此，外包数据的安全性保证仍然是边缘计算数据安全的一个基础性问题。

到目前为止，国内外学者对边缘计算中数据安全的研究还处于探索阶段，大多数的研究成果都集中在其他计算环境下，例如云计算、移动云计算和雾计算等。因此，边缘计算中数据安全的一个主要研究思路是将其他计算范式下的数据安全方案移植到边缘计算范式中，并与边缘计算中并行分布式架构、终端资源受限、边缘大数据处理、高度动态环境等特性进行有机结合，最终实现轻量级、分布式的数据安全防护体系。本节主要从数据保密性与安全数据共享、完整性审计和可搜索加密这 3 个方面展开综述，选取了其他计算范式中的部分重点成果进行介绍和分析，进而映射出在边缘计算环境下的研究方向，并给出研究建议。

3.1　数据保密性与安全数据共享

现有的数据保密性和安全数据共享方案通常采用加密技术来实现，其常规流程是由数据所有者预先对外包数据进行加密处理和上传操作，并在需要时由数据使用者解密。传统的加密算法包括对称加密算法（如 DES、3DES、ADES 等）和非对称加密算法（如 RSA、Diffe-Hellman、ECC 等），但传统加密算法加密后的数据可操作性低，对后续的数据处理造成很大阻碍。目前比较常用的数据加密算法有基于属性加密（ABE）、代理重加密（PRE）和全同态加密（FHE）算法等。

3.1.1　属性加密算法

属性加密[12]（ABE, attribute-based encryption）是一种控制接收者对加密数据的解密能力的密码机制，当用户所拥有的属性满足一定的接入策略时，就可以解密信息，接入策略可以用逻辑表达式表示，也可以转化为树型结构。即使是一种基于属性的门限策略，只有用户属性集与密文属性集相交的元素数量达到系统规定的门限参数时才能解密。ABE 可以分为基于密钥策略的属性加密（KP-ABE）[13]和基于密文策略的属性加密（CP-ABE）[14]，两者分别能够实现接收方制定访问控制策略和发送方规定访问控制策略。

基于密文策略的属性加密方案被广泛应用于云计算中数据存储和共享安全中，传统的 CP-ABE 方案往往通过构造单调访问树结构并嵌入密文中，只有用户的属性集合满足访问树对应的门限要求时才能够访问密文。但在实际的数据存储场景中，共享的数据文件通常具有多层次特征，因此单调访问树结构无法满足多层文件数据的细粒度访问共享。针对这一问题，Wang 等[15]提出了一种高效的

基于文件分层结构的加密方案，将分层访问结构集成到单一属性访问结构中，然后通过集成后的访问结构对分层文件进行加密，大大提高了数据的存储安全性。虽然属性加密方法能够实现可扩展数据存储和细粒度数据共享，但其在属性撤销方面的支持性较差，因此，Yang 等[16]针对属性加密方法中用户属性撤销这一挑战性问题，给出了解决方案。通过引入扩展的“代理—辅助”方法和“全或无”原则，削弱云服务器在用户属性撤销操作过程中的决策权限，从而有效防御云服务器与恶意第三方的合谋攻击。Zuo 等[17]在雾计算环境下构建了具有外包解密的属性加密方法（OD-ABE），最后证明该方案是选择密文攻击（CCA）安全的。

3.1.2 代理重加密算法

代理重加密（PRE）是由 Blaze 等[18]在 1998 年的欧洲密码学年会上提出的，在 PRE 中，一个半可信的代理者能够利用重加密密钥（re-encryption key）将原本针对数据拥有者公钥的密文转换成针对数据使用者公钥的密文，并可以保证该代理者无法获知对应明文的任何消息。因此，代理重加密被广泛应用于数据转发、文件分发等多用户共享的云安全应用中。

随后，一系列基于代理重加密的密码算法被陆续提出，例如，2007 年提出的基于身份的代理重加密方案[19]（IBPRE），该方案将用户的身份信息作为公钥参与重加密过程，使重加密密钥具有单向性；2009 年，Weng 等[20]提出了条件代理重加密算法（CPRE），只有当转换密文符合某种既定条件时，代理才可以成功地对该密文进行转换，相对于传统的代理重加密，条件代理重加密能够更好地控制代理者的转换权限，因此，更适合于实际应用场景。

由于代理重加密的密文转换和权限控制特性，通常与其他加密方法结合使用。Liang 等[21]提出一种基于密文策略的属性代理重加密方案（CP-ABPRE），在基于属性加密的密码设置中采用 PRE 技术，这样就使代理能够将一种访问策略下的加密转换为另一种新访问策略下的加密。此外，该方案将双系统加密技术与选择性验证技术相结合，证明了 CP-ABPRE 是不可区分性选择密文攻击（IND-CCA）安全的。Yang 等[22]在文献[21]的基础上进一步改进了 CP-ABPRE 方案，首次将条件代理重加密 CPRE 与属性加密 ABE 相结合，提出一种基于密文策略的属性条件代理重加密方案，并通过 CPRE 中代理权限控制特性，实现安全的用户属性撤销。2016 年，Shao 等[23]在动态云存储环境下构建了一种具有固定密文长度的双向代理重加密方案（BPRE），密文长度与转换次数无关，并基于随机预言机困难模型证明了其在选择密文攻击下是可重放安全（RCCA）的。Khan 等[24]提出一种基于云和代理的双重加密方案（CMReS），其结合了基于代理的重加密和基于云的重加密特性，能够将计算密集型任务迁移到云计算中心，实现移动终端的最小化计算成本。2017 年，Khan 等[25]对 CMReS 方案进行了进一步拓展，针对可信实体与移动终端之间的任务迁移问题，提出了一种基于重加密的工作负载分配模型，实现移动终端的最小计算负载，提高了整体性能。

3.1.3 全同态加密算法

全同态加密（FHE, fully homomorphic encryption）最早是由 Rivest 等[26]于 1978 年提出的一种基于数学难题和计算复杂性理论的密码学技术。其计算特性在于对明文进行代数运算再加密，与加密后对密文进行相同代数运算的结果是等价的。随后全同态加密方法经历了几个发展阶段，2009 年，Gentry[27]构造出了第一个基于多项式环上理想格的全同态加密方案，支持加法同态和乘法同态（任意多项式时间的计算）并且具有语义安全性，但是该方案的计算复杂度高，加解密效率低。在 2010 年的欧洲密码学年会上，Dijk 等[28]提出基于近似最大公因子困难问题的全同态加密算法（DGHV），相比于 Gentry09 方案，它采用基于整数加密的模块化算数来代替理想格上的复杂运算，但缺陷在于其公钥的长度仍然很长。2011 年，Brakerski 等[29]结合模交换和密钥交换技术成功构造了基于纠错学习问题（LWE）的同态加密方案。2013 年，Gentry 等[30]在文献[29]的基础上提出了一个基于近似特征向量的全同态加密方案，该方案的优势在于不需要使用模交换和密钥交换技术就能够实现全同态加密，大大提高了算法效率。Louk 等[31]在移动多云计算环境下构造了同态加密算法，为移动用户提供数据安全防护。Baharon 等[32]针对同态加密中的计算效率问题进一步提出了轻量级同态加密算法（LHE），在实现加法同态和乘法同态的同时最小化加密和密钥生成时间。表 1 从方案的分类、技术方法、安全模型、安全特性和可扩展性等方面对上述解决方案进行了总结。

表 1　　现有数据保密性与安全数据共享方案

文献	分类	方案	技术方法	安全模型	安全特性	可扩展性
文献[15]	属性加密	基于文件分层结构的属性加密方案	基于密文的属性加密、分层访问树	选择明文攻击	数据保密性、细粒度数据共享	高
文献[16]		支持用户属性撤销的属性加密方案	基于密文的属性加密、全或无原则	选择明文攻击	数据保密性、支持用户属性撤销、抵抗合谋攻击	中等
文献[17]		支持外包解密的属性加密方案	属性加密方法	选择密文攻击	数据保密性、安全存储	高
文献[21]	代理重加密	基于密文策略的属性代理重加密方案	基于密文的属性加密、代理重加密	不可区分性选择密文攻击	细粒度数据共享	高
文献[22]		基于密文策略的属性条件代理重加密方案	基于密文的属性加密、条件代理重加密	选择明文攻击	支持用户属性撤销、细粒度数据共享	中等
文献[23]		固定密文长度的双向代理重加密方案	双向代理重加密	可重放选择密文攻击	安全存储、抵抗合谋攻击	高
文献[24]		基于云和代理的双重加密方案	代理重加密	无	数据保密性、计算迁移	中等
文献[25]		基于重加密的工作负载分配模型	代理重加密	无	数据保密性、计算迁移	高
文献[31]	全同态加密	移动多云计算环境下的同态加密构造方案	全同态加密	无	数据保密性、安全存储	高
文献[32]		轻量级同态加密算法	全同态加密	蛮力攻击	数据保密性、安全存储	高

3.2　完整性审计

当用户的数据存储到边缘或云数据中心之后，一个重要的问题就是如何确定外包存储数据的完整性和可用性。目前对数据完整性审计相关的研究主要集中在以下 4 点功能需求上[33]。

1) 动态审计。数据存储服务器中的用户数据往往是动态更新的，常见的动态数据操作包括修改、复制、插入和删除等，因此，数据完整性审计方案不能仅局限于静态数据，而应当具有动态审计功能。

2) 批量审计。当有大量用户同时发出审计请求或数据被分块存储在多个数据中心时，为了提高审计效率，完整性审计方案应具备批量审计的能力。

3) 隐私保护。由于数据存储服务器和数据所有者都不适合执行完整性审计方案，因此，往往需要借助在第三方审计平台（TPA）来构建。在这种情况下，当 TPA 为半可信或不可信时，极有可能发生数据泄露和篡改等安全威胁，数据隐私将无法保证。因此，在完整性审计的过程中保护用户数据隐私是必不可少的。

4) 低复杂度。由于数据存储服务器（边缘数据中心）和数据所有者（边缘设备）存在计算能力、存储容量、网络带宽等方面的限制，因此在设计完整性审计方案时除了保证数据完整性之外，方案的复杂度问题也是一个重要因素。

Wang 等[34]针对数据完整性审计过程中的隐私泄露和批量审计问题，提出了一种保护隐私的分布式数据审计系统。系统采用第三方审计平台执行完整性审计工作，数据所有者将数据外包存储到云服务器之后即可删除本地原始数据，同时利用同态认证器和随机掩码技术来保证第三方审计平台在有效的审计过程中无法获知存储数据的内容，实现隐私保护。其次，考虑到 TPA 的批量审计特性，利用双线性聚合签名方法进一步将协议扩展到多用户设置中，实现了分布式多任务审计。随后，Wang 等[35]进一步对文献[34]中的方案进行改进，通过构造基于块认证标签的 Merkle 散列树型结构来改进存储模型的证明。文献[35]进一步改进了双线性聚合签名方法，提高了 TPA 的批量审计效率。Yang 等[36]首先分析了现有的远程数据审计技术（RDA）仅适用于静态数据，而不适用于动态数据更新的不足，随后提出了一个高效的、隐私保护的动态审计协议。方案采用密码技术与双线性对中双线性性质相结合的方式来代替随机掩码技术，实现隐私保护。同时将方案扩展，实现动态数据操作和批量审批，并给出了该方案在随机预言机模型下的安全性证明。Sookhak 等[37]在文献[36]的基础上提出了一种基于代数签名特性的高效 RDA 技术，实现了最小的计算和通信成本。该文通过构建一种适用于大规模数据存储的数据结构 DCT 来有效地支持块级动态数据操作，如插入、修改和删除，而不需要下载整个数据文件。文献[38]针对移动终端设备中计算能力的不足，提出了 2 种轻量级的隐私保护完整性

审计协议：基础协议和改进协议。基础协议基于在线/离线签名方法，支持在外包数据之前进行离线式签名计算处理，而当给定要外包的数据文件时，用户只需执行轻量级计算来构建在线阶段外包的数据签名即可。文献[38]进一步对基础协议进行扩展，使用 Merkle 散列树型认证结构来改进基础协议中的部分签名正确性，以支持批量审计和动态操作。数据持有性证明（PDP）是另一种提供数据持有性概率保证的完整性审计方法，但该方法在完整性验证过程中需要访问所有数据块，造成了过高的计算复杂性和存储空间消耗。针对这个问题，Lin 等[39]在移动云计算环境下提出了 2 种移动数据可持有性证明方案（MPDP），通过构造基于散列树的数据结构来支持动态数据操作，同时结合 BLS 短签名方法实现高效率、低复杂度的完整性审计。表 2 从方案的分类、技术方法、应用场景、安全特性和可扩展性等方面对上述解决方案进行了总结。

3.3 可搜索加密

在传统的云计算范式中，为了在实现数据安全性的同时降低终端资源消耗，用户往往采用某种加密方式将文件加密外包给第三方云服务器。但是当用户需要寻找包含某个关键字的相关文件时，将会遇到如何在云端服务器的密文上进行搜索操作的难题。为了解决此类问题，可搜索加密（SE, searchable encryption）应运而生，SE 可以保障数据的私密性和可用性，并支持对密文数据的查询与检索。同样地，在边缘计算范式中，用户的文件数据也会被加密外包到边缘计算中心或云服务器中，可搜索加密也是边缘计算中保护用户隐私的一个重要方法。可搜索加密方案的一个典型问题在于其算法的复杂度过高，执行过程中会产生大量功耗，这类弊端在面向物联网的边缘计算中尤为突出。因此，如何从算法的复杂度出发，设计一种高效的、适合边缘设备和隐私保护的可搜索加密方案是一个重要研究点。

3.3.1 安全排名可搜索加密

安全排名搜索是指系统按照一定的相关度准则（如关键字频率）将搜索结果返回给用户。安全排名搜索提高了系统的适用性，符合边缘计算环境下的隐私数据保护的实际需求。

Wang 等[40]在对称可搜索加密（SSE）的基础上首次提出了一种安全排名对称可搜索加密（RSSE）算法，利用关键字频率和反向索引策略来度量关键字与密文数据之间的相关程度，实现云计算下安全排名的加密搜索。此外，文章还设计了一种新的密码原语 OPSE（order preserving symmetric encryption），利用一对多的保密映射来保护用户的数据隐私，同时能够对用户返回的搜索结果进行验证。Cao 等[41]在文献[40]的基础上，考虑了一种多关键字的排名搜索算法（MRSE），该算法能够按照关键字顺序返回对应文件，通过在各关键字语义中构建“协调匹配”的有效相似性度量，来尽可能多地匹配以捕获数据文件与搜索关键字的相关性，同时结合“内积相似度（inner product similarity）”对相关性进行定量评估。值得一提的是，上述 2 种方案均面临搜索效率较低的问题，当系统的用户数量过多时，方案的搜索效率会大幅降低。

针对安全排名可搜索加密的搜索效率问题，Li 等[42]在移动云计算环境下，利用同文献[41]一样的相关性方法，引入 K 最近邻（K-NN）技术实现了移动云计算环境下的高效多关键字安全排名搜索系统（EMRS），且能够保证返回结果的准确性。该系统采用高效的索引结构来提高搜索效率，同时，采用盲存储（blind storage）系统来隐藏搜索用

表 2 现有完整性审计方案综合比较

研究文献	分类	方案	技术方法	应用场景	安全特性	可扩展性
文献[34]	批量审计	保护隐私的批量数据审计系统	同态认证器、随机掩码、双线性聚合签名	云计算	批量审计、隐私保护	高
文献[35]	动态审计	支持动态审计的安全云存储方案	Merkle 散列树、数据持有性证明	云计算	动态审计、安全存储	高
文献[36]	动态审计	高效隐私保护的动态审计方案	远程数据审计技术	云计算	动态审计、隐私保护	中等
文献[37]	动态审计	动态远程数据审计方案	远程数据审计、分治表	大数据存储	动态审计、低复杂度	中等
文献[38]	批量审计	适用于资源受限终端的隐私保护审计方案	在线/离线签名方法	移动云计算	批量审计、隐私保护、低复杂度	高
文献[39]	动态审计	移动数据可持有性证明方案	可持有性证明、BLS 短签名	移动云计算	动态审计、低复杂度	高

户的访问模式，实现隐私保护，最后通过仿真实验表明 EMRS 能够实现比 MRSE 更高效率的多关键字安全排名搜索。文献[43]提出了一种通信和能量节约的加密搜索方案（TEES），在实现隐私保护可搜索加密的同时提高搜索效率，所设计的搜索框架能够将大量计算任务迁移到云端，缩短了 23%~46%的计算时间，且每个文件的搜索能耗下降了 35%~55%，适用于带宽、存储和计算资源受限的移动终端，且具有高扩展性。

3.3.2　基于属性的可搜索加密

基于属性的可搜索加密能够在实现有效搜索操作的同时支持细粒度的数据共享。2013 年，Wang 等[44]提出了一种具有关键字搜索功能的 CP-ABE 方案（KSF-CP-ABE），通过构建一种与加密数据相同访问策略的关键字检索系统，使只有满足访问策略的授权用户才能通过关键字搜索得到密文数据，实现细粒度的搜索控制。该文献还给出了基于双线性对的构造方案，该方案的高效性在于云端的搜索过程只需要 3 次双线性对操作，而用户的解密过程仅需要一次双线性对即可完成，并且能够抵御内部和外部攻击者的攻击，实现隐私保护。

2014 年，Zheng 等[45]将用户的搜索权限问题进行定义，指出一个授权用户应具有搜索、外包和验证这 3 类功能权限，并就如何保证这 3 类功能权限的正确执行，提出了一种可验证的基于属性的公钥可搜索加密方案（VABKS），该方案允许数据所有者根据访问控制策略控制其外包加密数据的搜索和使用，同时允许合法用户将搜索操作外包给云服务器，并能够验证云服务器是否能够准确地执行搜索操作和返回结果的正确性。同年，Liu 等[46]指出 VABKS 方案的实用性问题，其构造方法必须要通信双方建立安全信道。针对这个问题，作者提出了一种基于密钥策略属性加密的关键字搜索方案（KP-ABKS），不需要建立安全信道就能实现安全搜索，且能够有效抵御离线关键字猜测攻击。

2016 年，Sun 等[47]考虑了一种外包数据集由多个所有者提供和多个数据使用者搜索的场景（multi-user multi-contributor case），提出了一种具有高效用户撤销功能的基于属性的关键字搜索方案（ABKS-UR）。该方案具有高效的用户撤销功能，实现了可扩展的细粒度搜索授权，且允许多个数据所有者独立地将其数据加密和外包给云服务器，数据使用者可以生成自己的搜索功能，而不依赖于第三方可信机构。同时，引入代理重加密和懒惰重加密（lazy re-encryption）技术将用户撤销操作中的更新工作委托给云服务器。最后证明了该方案能够抵抗选择关键字攻击。

3.3.3　支持动态更新的可搜索加密

需要指出的是，在实际的加密数据搜索过程中，密文数据往往是动态更新的。传统的静态搜索方法仅对固定密文有效，当密文数据经过删除或增加操作后，就需要重新构造搜索信息。与之相反，动态可搜索加密方案能够有效支持密文数据的删除或增加操作，不需要重构搜索信息也能返回正确的搜索结果。

Kamara 等[48]基于对称可搜索加密方案（SSE）首次提出了动态对称可搜索加密（DSSE）的概念，允许用户存储一个动态的加密数据文件到服务器上，并支持在此文件上执行关键字搜索，给出了 DSSE 的一个严格安全性定义：抵抗适应性选择关键字攻击（CKA2），并给出了证明过程。该方案通过构造紧凑的索引结构来支持高效数据更新，包括删除、修改和增加。首先，通过引入额外的删除数组和相应的速查表来快速定位被删除密文的数据指针，进而实现快速删除；其次，数据修改功能则通过在数据指针上构建同态加密来实现；最后，通过在搜索数组中增加额外的空间表结构来实现新数组节点的加入。DSSE 在满足 CKA2 安全性的同时提供数据更新功能，但是该方案的计算复杂度很高，难以实现，并且在更新数据时很可能泄露隐私。针对上述问题，文献[49]中引入基于红黑树的索引结构，提出了 DDSE 的并行实现方法，算法执行时间与服务器数量成反比，使 DSSE 能够支持多处理器并行处理，大大提高了密文数据的搜索和更新效率。

Sun 等[50]提出了一种有效的可验证的连接关键字搜索方案（VCKS），该方案同时支持连接关键字搜索、动态数据更新和搜索结果验证。其中，搜索结果验证机制允许用户将搜索任务委托给云服务器，由云服务器中的公共信任机构（TA）来处理，也可以利用双线性映射累加器技术构建认证数据结构，由用户执行。Xia 等[51]提出了一种支持动态更新操作的安全多关键字排名搜索方案。该方案结合向量空间模型和通用的 TF-IDF 模型来构造一种树型索引结构（tree-based index structure），进一步

采用树型索引结构和“贪心深度搜索（greedy depth-first search）”算法来提供高效的多关键字排名搜索。此外，方案还引入了 *K*-NN 算法来加密索引和搜索向量，同时保证了索引和搜索向量之间的准确相关性计算。由于该方案使用了特殊的关键字平衡二叉树作为索引结构，因此，搜索时间能够呈亚线性，同时具备灵活的文件删除和插入的能力。Hu 等[52]指出基于属性的关键字搜索方案（ABKS）仅能够实现细粒度的搜索授权，但无法有效地更新搜索权限。针对这个问题，该文献提出了一种基于动态属性的关键字搜索方案（DABKS），将代理重加密（PRE）和秘密共享方案（SSS）相结合，实现了细粒度搜索授权和访问策略的高效更新，但缺陷在于只支持单一关键字搜索。

3.3.4 可搜索代理重加密

2010 年，Shao 等[53]将代理重加密（PRE）方案与具有关键字搜索功能的公钥加密方案（PEKS, public encryption with keyword search）相结合，首次提出了可搜索代理重加密（PRES, proxy re-encryption with keyword search）的概念，并成功构造出了一种可证明安全的双向 PRES 方案，实现搜索和解密的第三方代理协议。同时，在决策双线性 Diffie-Hellman 假设（DBDH）和随机预言机模型下证明了该协议的安全性。最后给出了 PRES 方案在云计算和传感器网络下的应用实例。

2012 年，Wang 等[54]在文献[53]的工作基础上，进一步扩展了 PRES 方案，提出了一种支持连接关键字搜索的约束单向单跳代理重加密方案（CPRE-CKS），相比于 PRES 方案中代理方可以重加密所有的二级密文，CPRE-CKS 则只能重加密包含相应关键字的二级密文，在支持连接关键字搜索的同时提升搜索效率。文献[54]还给出了基于双线性对的构造方案，并在随机预言机模型下证明了该方案的安全性。但 CPRE-CKS 方案的缺陷在于其只满足弱选择密文攻击安全性（wCCA）。针对这个安全性问题，Fang 等[55]将条件代理重加密机制与公钥可搜索加密机制相结合，提出了一种支持关键字搜索的条件代理重加密方案（C-PRES）。通过关键字匿名方式实现了方案的选择密文攻击安全性。

2014 年，Shi 等[56]提出了一种支持关键字搜索的属性代理重加密方案（ABRKS），将属性加密（ABE）和代理重加密（PRE）相结合，以细粒度的访问控制方式进行关键字搜索。此外，该文还给出了 ABRKS 在 CP-ABE 和 KP-ABE 下的不同构造方案，并且在随机预言机模型和决策多线性 Diffie-Hellman 假设（MDDH）下证明了方案安全性。表 3 从方案的分类、技术方法、对称性、安全模型、功能性和可扩展性等方面对上述解决方案进行了总结。

3.4 研究方向展望

综上所述，数据加密技术为保证各类计算模式中的数据安全提供了有效的解决办法。在开放式的边缘计算环境下，如何将传统的加密方案与边缘计算中并行分布式架构、终端资源受限、边缘大数据处理、高度动态环境等特性进行有机结合，实现轻量级、分布式的数据安全防护体系是未来的重点研究内容。

1) 在数据保密性和安全数据共享方面，结合属性加密、代理重加密和同态加密等应用加密理论，如何设计低时延、支持动态操作的分布式安全存储系统和正确处理网络边缘设备与云中心之间的协同性是一个重要的研究思路。

2) 在数据完整性审计方面，一个主要的研究目的在于实现各种审计功能的同时尽可能提高审计效率并降低验证开销。其次，设计支持多源异构数据和动态数据更新的完整性审计方案有望成为未来的研究重点。

3) 在可搜索加密方面，首先，如何在分布式存储服务模型下构造基于关键字的搜索方案，进一步拓展至边缘计算环境中是一个可行的研究思路；其次，如何在安全多方共享模式下实现细粒度的搜索权限控制，使其在适用于不同信任域的多用户搜索环境的同时，保证搜索的速度和精度。最后，针对边缘计算中分布式密文数据存储模型，如何高效地构造安全索引使其适用于资源受限的网络边缘设备以及设计分布式可搜索加密算法是一个亟待解决的问题。

4 身份认证

边缘计算中通常包含多个功能实体，如数据参与者（终端用户、服务提供商和基础设施提供商）、服务（虚拟机、数据容器）和基础设施（如终端基础设施、边缘数据中心和核心基础设施）。因此，边缘计算是一种多信任域共存的分布式交互计算系统。在这种复杂的多实体计算范式下，不仅需要

表 3　　现有可搜索加密方案比较与分析

研究文献	分类	方案	技术方法	对称性	安全模型	功能性	可扩展性
文献[40]	安全排名关键字搜索方案	云数据的安全排名关键字搜索	保序对称加密、反向映射	对称	无	排名搜索	中等
文献[41]		多关键字排名搜索	协调匹配、内积相似度	对称	无	多关键字	中等
文献[42]		移动云环境下多关键字排名搜索	*K*-最近邻、盲存储	对称	无	多关键字	高
文献[43]		移动云环境下高效的排名搜索	计算迁移技术	对称	无	高效搜索	高
文献[44]	基于属性的加密搜索方案	支持关键字搜索的 CP-ABE 方案	属性加密、秘密共享	非对称	无	搜索控制	高
文献[45]		基于属性的可验证加密搜索	属性加密	非对称	无	可验证性	高
文献[46]		基于 KP-ABE 的可搜索加密	属性加密、公钥加密	非对称	离线猜测攻击	可验证性	中等
文献[47]		支持用户撤销的可搜索加密	属性加密、代理重加密	非对称	不可区分性选择关键字攻击	搜索授权	高
文献[48]	支持动态更新的可搜索加密	动态可搜索对称加密	动态可搜索对称加密、随机掩码技术	对称	适应性选择关键字攻击	动态搜索	中等
文献[49]		并行的动态可搜索对称加密	红黑树索引结构	对称	适应性选择关键字攻击	动态搜索	高
文献[50]		可验证的动态连接关键字搜索	双线性映射累加器	非对称	通用可组合	动态搜索	高
文献[51]		动态多关键字排名搜索	*K*-最近邻、贪心深度搜索算法	非对称	唯密文攻击	动态搜索 多关键字 排名搜索	高
文献[52]		基于动态属性的关键字搜索	属性加密、代理重加密	非对称	选择关键字攻击	动态搜索	中等
文献[53]	可搜索代理重加密	支持关键字搜索的代理重加密	代理重加密	非对称	选择密文攻击	代理搜索	高
文献[54]		支持连接关键字搜索的单跳代理重加密	代理重加密	非对称	弱选择密文攻击	连接关键字搜索	中等
文献[55]		支持关键字搜索的条件代理重加密	条件代理重加密	非对称	选择密文攻击	代理搜索	高
文献[56]		支持关键字搜索的属性代理重加密	属性加密、代理重加密、线性秘密共享	非对称	选择关键字攻击	代理搜索	高

为每个实体分配一个身份，而且还需要允许不同信任域之间的实体进行相互验证。同时，考虑到终端设备的高移动特性，切换认证技术也是身份认证协议中的一个重要研究点。

4.1　单一域内的身份认证

单一信任域内的身份认证主要用于解决每个实体的身份分配问题，各实体首先要通过授权中心的安全认证才能够获取存储和计算等服务。随着研究的深入开展，设计具有隐私保护特性的身份认证协议是当前的研究重点。

2015 年，Liu 等[57]提出了一种基于共享权限的隐私保护认证协议 SAPA，同时解决了云存储中的隐私问题。该方案通过匿名访问请求匹配机制实现访问权限的共享，同时采用基于属性的访问控制机制来限制用户字段的访问权限，而多用户之间的数据共享则通过代理重加密来实现。最后给出了 SAPA 的通用组合（UC）模型，证明了 SAPA 的正确性。同年，文献[58]在分布式云服务环境中提出了一种保护隐私的匿名身份认证方案，其安全性基于双线性配对密码系统和动态随机数生成。此外，该方案还支持相互认证、密钥交换、用户匿名和不可追踪性。2016 年，Jiang 等[59]指出文献[58]中的方案不能抵抗服务提供商的伪造攻击，即敌手可以伪造任何服务提供商对用户进行身份认证，从而对相互认证的支持性较弱，并给出了进一步的研究建议。同年，He 等[60]进一步分析了文献[58]中身份认证方案的不足之处，指出该方案不仅不能抵制伪造攻击，而且敌手在发起伪造攻击的过程中能够提取用户的真实身份，从而获取用户隐私。针对上述问题，He 等提出了一种基于身份签名的隐私认证方案 PAA，并给出了 PAA 的安全性证明和对比分析。Lo 等[61]针对车辆传感器网络（VSN）提

出了一种基于条件隐私的身份认证方案。该方案采用椭圆曲线加密（ECC）机制和基于身份的签名机制，支持匿名认证、数据完整性、可追溯性和批量签名验证，同时，签名过程中不需要任何双线性对的操作，能够大幅度节约时间消耗和计算成本。Mahmood 等[62]针对智能电网系统提出了一种基于轻量级 ECC 的认证方案。在抵御所有已知的安全攻击的同时实现了低计算量和通信成本的相互认证。

4.2 跨域认证

目前，适用于不同信任域实体之间的认证机制研究还处于初级阶段，尚未形成较为完善的研究脉络和理论方法。在云计算的身份认证研究中，多个云服务提供商之间的身份管理可以看作是一种跨域认证形式，这就使一些适用于多云之间的认证标准（如 SAML、OpenID 等）以及单点登录（SSO）认证机制有希望应用于多信任域之间的身份认证[63]。文献[64]针对结构化 P2P 网络设计了一种基于属性的认证授权框架，该框架采用属性证书和分布式证书撤销系统，来代替传统 P2P 网络中公钥证书和访问控制列表的认证机制，能够实现灵活、高效率和隐私保护的权限分配，且不需要任何外部干预的服务器或第三方可信机构。文献[65]以电子医疗（e-health）为背景，提出一种跨域的动态匿名组密钥管理认证系统（CD-AGKMS），该系统通过建立以密钥生成中心（KGC）为最顶层的树型层次结构，实现跨域组密钥协商。同时，在组密钥管理方面，该方案提供由时间控制的密钥撤销机制，用户的密钥在有效时间段到期时被撤销。此外，CD-AGKMS 不需要双线性对的计算，提高了系统的可行性和高效性。由于这些方法的设计与边缘计算中的底层基础设施互相兼容，所以这些方法都有可能适用于处理属于不同信任域的边缘数据中心的身份认证机制中。

4.3 切换认证

由于边缘计算中终端设备的高移动性，移动用户的地理位置经常发生变化，使传统的集中式身份认证协议不再适用于此类情况。而切换认证就是为了解决高移动性用户身份认证的一种认证移交技术，因此，对切换认证技术的研究能够为边缘计算中边缘设备的实时准确认证提供有力保障，同时在认证移交过程中的用户身份隐私问题也是一个研究重点。

Yang 等[66]基于异构移动云网络提出了一种切换认证协议，协议采用基于身份的椭圆曲线算法，解决了移动云计算中认证移交过程中的隐私问题，实现了认证匿名性和不可追踪性。但是该协议通常需要访问位于集中式云基础设施中的身份认证服务器，因此，仍有改进空间。值得一提的是，由于边缘计算允许用户部署自己的个人数据中心，因此，一些私有云平台的认证协议有希望应用到边缘计算中。其中，一个典型的私有云平台认证框架是 OPENi[67]，该框架提供了对外部用户的访问权限认证协议，认证组件使用 OpenID Connect 身份验证层以及其他验证机制，使云端所有者能够决定哪些认证服务器是可信的以及允许哪些用户有访问云端资源的权限。He 等[68]综述了过去几年里应用于移动无线网络的切换认证协议，指出移动无线网络中的切换认证协议应满足 8 个安全和隐私要求，该文在移动设备上对几种典型协议进行了实现，分析结果指出使用椭圆曲线算法（ECC）的切换协议具有最低的计算成本，但使用 ECC 的安全协议不能支持批量认证。针对这一问题，该文作者采用基于身份的公钥密码技术（PKC），设计了一种适用于移动无线网络的隐私保护切换认证协议，在保护用户身份隐私的同时，实现了批量认证功能。表 4 从方案的分类、技术方法、应用场景、安全特性和可扩展性等方面对身份认证的各类解决方案进行了总结。

4.4 研究方向展望

当前，国内外研究者对身份认证协议的研究大多是在现有的安全协议基础上进行改进和优化，包括协议的灵活性、高效性、节能性和隐私保护等。在边缘计算中，身份认证协议的研究应借鉴现有方案的优势之处，同时结合边缘计算中分布式、移动性等特点，加强统一认证、跨域认证和切换认证技术的研究，以保障用户在不同信任域和异构网络环境下的数据和隐私安全。

由于边缘计算是一个多实体和多信任域共存的开放式动态系统，因此身份认证协议要考虑到实体与信任域之间的对应关系。具体的研究内容包括同一实体在不同信任域之间的跨域认证和切换认证；不同实体在相同信任域内的身份认证和相互认证；最后，在实现轻量级身份认证的同时兼顾匿名性、完整性、可追溯性和批量认证等功能也是一个重要的研究点。

表 4　　现有身份认证协议对比分析

研究文献	分类	方案	技术方法	应用场景	安全特性	可扩展性
文献[57]	单一域内身份认证	基于共享权限的隐私保护认证协议	属性加密、代理重加密	安全云存储	隐私保护、匿名认证	高
文献[58]		保护隐私的匿名身份认证方案	双线性密码系统	分布式移动云计算	匿名认证、密钥交换、不可追踪性	中等
文献[60]		基于身份签名的隐私感知认证方案	双线性密码系统	移动云计算	匿名认证、隐私保护、不可追踪性	高
文献[61]		基于条件隐私的身份认证方案	椭圆曲线密码系统	车辆传感器网络	匿名认证、可追溯性、批量签名验证	高
文献[62]		基于轻量级 ECC 的身份认证方案	椭圆曲线密码系统	智能电网系统	双向认证、低计算和通信成本	高
文献[64]	跨域认证	基于属性的认证授权框架	分布式证书撤销	结构化 P2P 网络	隐私保护、证书撤销	中等
文献[65]		跨域动态匿名组密钥管理认证系统	椭圆曲线密码系统	电子医疗系统	匿名认证、密钥撤销、隐私保护	中等
文献[66]	切换认证	基于身份的切换认证协议	椭圆曲线密码系统	异构移动云计算网络	匿名认证、隐私保护、不可追踪性	高
文献[68]		隐私保护的批量切换认证协议	椭圆曲线密码系统	移动无线网络	隐私保护、批量认证	高

5　访问控制

为了节省本地存储和计算成本，终端用户通常会将私有数据外包存储到边缘数据中心或云服务器中，数据的保密性很容易受到外部和内部攻击的威胁。因此，保密性和访问控制是确保系统安全性和保护用户隐私的关键技术和重要方法。传统的访问控制方案大多假设用户和功能实体在同一信任域中，并不适用于边缘计算中基于多信任域的授权基础架构。因此，边缘计算中的访问控制系统在原则上应适用于不同信任域之间的多实体访问权限控制，同时还应考虑地理位置和资源所有权等各种因素。

5.1　基于属性的访问控制

由于边缘计算是以数据为主导的计算模式，因此，边缘计算的访问控制通常采用密码技术来实现，传统的密码技术并不适用于分布式并行计算环境，而属性加密（ABE）能够很好地适用于分布式架构，实现细粒度数据共享和访问控制。

Yu 等[69]将基于密钥策略的属性加密 KP-ABE 和代理重加密 PRE 相结合，首次提出了一种安全、可扩展和细粒度的数据访问控制方案，其中 KP-ABE 能够实现细粒度访问控制，PRE 用于用户属性撤销和计算成本迁移，并在标准模型下证明了方案的安全性，为基于属性的访问控制方案的研究奠定了理论基础。传统基于属性的访问控制大多为单一属性授权方式，这种构造方式的缺陷在于在进行访问控制的同时必须执行用户合法性验证和密钥分发，在大规模的分布式计算模式下，极易导致单点性能瓶颈问题，使整个访问控制系统执行效率十分低下。因此单一属性授权方的构造方式并不适用于边缘计算。针对这个问题，Xue 等[70]提出了一种顽健和可审计的访问控制方案（RAAC），方案采用支持多属性授权访问控制的异构框架，能够有效地消除单点性能瓶颈问题。该框架的创新之处在于设计了多个属性授权方来共享用户合法性检验和密钥分发的负载，同时每一个授权方都能够单独地管理整个属性集，在消除单点性能瓶颈的同时提高了效率。最后还给出了一个审计机制，用于检测合法性验证的执行情况。

近几年，随着移动云计算和雾计算的深入研究，一些兼顾安全性、高效性和轻量级的访问控制方案被陆续提出。Jin 等[71]在移动云计算环境下提出一种基于 CP-ABE 的轻量级数据访问控制方案（SL-CP-ABE），能够保护外包数据的机密性，并在移动云中提供细粒度的数据访问控制。该方案通过减少加解密操作次数来降低计算开销，从而显著地提高系统性能，适用于轻量级移动设备。Zhang 等[72]在文献[71]的基础上，提出了一种具有外包能力和属性更新的访问控制策略，该策略同样采用 CP-ABE 方案实现细粒度访问控制，同时将访问结构和属性相关的加解密操作外包到雾节点，使加解密操作所对应的访问结构和密钥更新与数据所有者无关，适用于终端资源受限的智能设备。该

文最后在决策双线性 Diffie-Hellman 假设下证明了该策略的安全性。Huang 等[73]进一步扩展了访问控制策略中的更新能力，提出一种具有计算外包和密文更新的访问控制方案，方案采用属性签名技术（ABS）来实现密文更新，授权用户在签名中集成了自己的属性集合，当满足既定的更新策略时，才能够进行密文更新操作。文献[73]沿用了文献[72]中的计算外包方法，将大量加解密相关的双线性对操作外包到雾节点中，最小化终端的计算成本。

5.2 基于角色的访问控制

基于角色的访问控制通过双重权限映射机制，即用户到角色和角色到数据对象上的权限映射来提供灵活的控制和管理。

Zhou 等[74]首先提出了一种基于角色的加密方案（RBE），该方案能够始终保持固定的密文大小和解密密钥，并且支持用户撤销。随后将该加密方案应用到访问控制策略中，进而提出了一种基于角色加密的混合云存储构架，该构架允许用户在公共云中安全地存储数据，同时保持与私有云中用户角色相关的敏感信息。Chen 等[75]指出传统的访问控制技术和方案无法满足庞大用户量的资源访问，进而提出了一种基于层次虚拟角色分配的协商 RBAC 方案，该方案支持多代理和多资源服务器协商管理访问控制权限，同时，方案还设计了一种有效的用户层次访问结构，并部署在代理或资源服务器中，能有效处理大量用户的资源访问请求。

Kuhn 等[76]首次将用户属性添加到基于角色的访问控制方案中，实现了动态角色分配和分布式访问控制，在快速认证的同时支持动态的权限管理。这种分布式访问控制架构在设计理念上十分符合边缘计算的要求，目前对分布式访问控制的研究大多集中在其他计算范式中[77]。文献[78]在多云环境中构建了基于角色的分布式访问控制策略，提供了域间角色映射和约束验证。这种方法很可能适用于边缘计算中的跨域实体间的访问控制策略。此外，还有一些其他的安全访问控制机制，虽然在设计之初并不是针对边缘计算的，但也有可能适合于边缘计算场景中。例如，带有属性协议的直接匿名认证方案[79]（DAA-A），该方案基于椭圆曲线加密系统 ECC，允许匿名用户证明他们拥有某种特定的可信属性。这些协议可以使用可信平台模块 2.0（TPM 2.0）规范中定义的原语进行实现，拥有 TPM 平台的用户可以选择向验证者显示的属性和隐藏的属性，同时采用零知识证明协议 ZKP 来验证隐藏属性的真实性。因此，该方案可以应用于 2 个边缘数据中心需要证明它们具有某些属性（如位置、功能）而不泄露其所有者的场景。表 5 从方案的分类、技术方法、应用场景和可扩展性等方面对各类访问控制方案进行了总结。

5.3 研究方向展望

综上所述，访问控制技术是确保系统安全性和保护用户隐私的关键技术和重要方法。边缘计算中的访问控制系统在原则上应适用于不同信任域之间的多实体访问权限控制，同时还应考虑地理位置和资源所有权等各种因素。因此，设计一种细粒度、动态化、轻量级和多域访问控制机制是接下来的研究重点，而高效的基于属性和角色的访问控制方法应该是比较适合边缘计算环境的技术手段。

表 5 现有访问控制系统分类对比

研究文献	分类	方案	技术方法	应用场景	可扩展性
文献[69]	基于属性的访问控制	细粒度的访问控制方案	属性加密、代理重加密	云计算	中等
文献[70]		支持多属性授权访问控制的异构框架	基于密文的属性加密	大规模云存储服务	高
文献[71]		安全和轻量级的属性访问控制方案	基于密文的属性加密	移动云计算	高
文献[72]		具有外包能力和属性更新的访问控制策略	基于密文的属性加密	雾计算	高
文献[73]		具有计算外包和密文更新的访问控制方案	基于密文的属性加密、基于属性的签名方法	雾计算	中等
文献[74]	基于角色的访问控制	基于角色加密的混合云存储架构	基于角色的加密方法	云存储服务	中等
文献[75]		基于层次虚拟角色分配的协商 RBAC 方案	层次加密、角色分层结构	大规模信息系统	高
文献[76]		基于角色-属性的访问控制方案	属性加密、角色加密	分布式云计算架构	高
文献[78]		基于角色的分布式访问控制	基于角色的加密方法	分布式云计算架构	高
文献[79]	TPM	带有属性协议的直接匿名认证方案	椭圆曲线密码系统、零知识证明	边缘计算	高

1) 支持跨域、跨群组的分级化访问控制方案，实现从单域到多域的细粒度访问控制，同时满足设计目标和资源约束将是未来的一个重要研究方向。

2) 跨域访问控制过程中的非法授权、访问冲突以及密钥管理、策略管理和属性管理等方面仍然存在很多亟待解决的问题。

6 隐私保护

边缘计算中的用户数据通常在半可信（honest-but-curious）的授权实体（边缘数据中心、基础架构提供商）中存储和处理，包括用户身份信息、位置信息和敏感数据等，这些半可信授权实体的次要目标在于获取用户的隐私信息，以达到非法盈利等目的。而在边缘计算这个开放的生态系统中，多个信任域由不同的基础架构提供商所控制，在这种情况下，用户不可能预先知道某个服务提供商是否值得信赖，因此，极有可能发生数据泄露或丢失等危及用户隐私的问题。

目前，对隐私保护的研究主要集中在移动云计算和雾计算环境中，本节从数据、位置和身份隐私这 3 个方面对近几年的隐私保护重点研究成果进行综述，以期对边缘计算中的隐私保护问题提供研究思路。

6.1 数据隐私保护

由于用户的私密性数据将由不在用户控制之下的实体进行存储和处理。因此，在保证用户隐私不被泄露的同时允许用户对数据进行各类操作（如审计、搜索和更新等）是当前的研究重点。

Pasupuleti 等[80]提出了一种针对移动设备的外包云数据隐私保护方案（ESPPA），该方案采用概率公钥加密技术（PPKE）和关键字排名搜索算法（RKS），在资源受限的移动终端上实现隐私保护的排名查询。首先，移动用户生成文件索引，并对数据和索引进行加密上传。其次，为了访问云中存储的密文数据，用户为关键字生成陷门并发送到云端。最终，云服务器根据搜索陷门向用户返回基于相关性得分的排序匹配数据，进而解密得到原始数据。Bahrami 等[81]在移动多云计算环境下提出了一种轻量级加密方法来存储云上的数据。该方法采用基于混沌系统的伪随机置换（PRPM）来实现轻量级加密，其置换操作是在移动设备上进行的，而不是在云端，从而保护数据隐私。Li 等[82]提出了一种隐私保护的数据利用系统，通过引入私有云代理（TPS）作为数据所有者/用户和公共云之间的访问接口，实现了精确的隐私保护关键字搜索和细粒度的访问控制。

6.2 位置隐私保护

随着基于位置服务的普及，位置隐私问题也成为了广为关注的研究点。目前，对本领域的研究重点主要集中于利用 K 匿名（K-anonymity）技术来实现位置服务中的隐私保护，但基于 K 匿名的位置隐私保护方案在实际应用中会消耗大量的网络带宽和计算开销，并不太适用于资源受限的边缘设备。因此，本文将介绍几种其他用于解决位置隐私问题的重要方法。

Chen 等[83]提出了一种基于分布式缓存推送的位置隐私保护方案。该方案引入了一种分布式缓存代理，用于将经常访问的位置相关数据存储在缓存代理中，并且将位置数据推送给移动用户。如果用户的位置数据在缓存数组中，则用户不会与基于位置的服务器进行通信，进而不会暴露自己的真实位置，实现位置隐私保护。Wei 等[84]在移动在线社交网络环境下设计了一种隐私保护的位置共享系统 MobiShare。该系统能够实现可信与不可信用户之间的位置共享，并支持范围查询和用户定义的访问控制。在共享过程中通过将用户身份和匿名位置信息分别存储在 2 个实体中，即使其中一个实体受到攻击，用户的位置隐私也能得到保护。Niu 等[85]提出了一种缓存感知的虚拟选择算法（CaDSA）来实现移动用户的位置隐私。在该算法中，移动设备向基于位置的服务提供商发送一些具有真实位置信息的虚假位置作为查询参数，使服务提供商无法发现用户的真实位置，实现位置隐私保护。同时，还提出了一种基于熵的隐私度量方法，将缓存命中率与隐私程度进行量化表示，从而实现缓存与隐私保护之间的定量分析。Fawaz 等[86]设计了一个名为 LP-Doctor 的细粒度访问控制工具，用于防止移动应用程序中位置服务带来的位置隐私威胁。LP-Doctor 是一种基于 Android 的移动设备工具，能够利用基于操作系统的位置访问控制，且不需要任何应用层或操作系统的修改。LP-Doctor 定义的功能组件包括应用程序会话管理器、策略管理器、位置检测器、移动管理器、威胁分析器和匿名执行器。当一个基于位置的应用程序启动时，应用程序会话管理器将应用程序启动和退出时间设置为匿名位置；策略管理器用于维护隐私政策，包括阻止、允

许和选择；位置检测器用于检测用户的当前位置，并且当用户位置改变时，移动管理器则更新用户的位置信息；威胁分析器根据策略管理器选取的隐私政策决定是否允许保护当前位置；如果威胁分析器决定保护位置信息，那么匿名执行器则采取相应的匿名措施，例如，增加一个虚假位置来确保位置匿名。

6.3 身份隐私保护

目前，对边缘计算范式中用户身份隐私的保护尚未引起广泛关注，仅有一些在移动云计算环境下的探索性研究成果。Khalil 等[87]指出当前的第三方身份管理系统（IDM）容易遭受 3 种攻击：IDM 服务器妥协、移动设备妥协和网络流量拦截。针对这些攻击问题，该文提出了一种综合的第三方身份管理系统（CIDM），该系统通过引入 IDM 服务器来代表服务提供商管理移动用户数字身份。首先，通过将授权凭证、IDM 服务器和服务提供商进行分离操作，来抵御非法访问 IDM 和流量拦截攻击；同时，添加额外的认证层以防止移动设备妥协。Khan 等[88]针对身份验证过程中的数字凭证泄露问题，提出一种基于动态凭证的轻量级身份隐私保护方案。该方案将身份认证动态凭证操作外包给第三方可信实体，以最小化移动设备的计算开销。此外，为了提高方案的性能和安全性，移动设备的凭证信息会根据移动云分组交换机制进行实时更新，以防止发生凭证窃取攻击。Park 等[89]在移动互联网服务中引入了改进的身份管理协议 I2DM。该协议采用基于公钥基础设施（PKI）的 PGP 算法，实现了用户身份管理和隐私保护。协议采用 256 bit 的加密密钥来保证会话安全性，并减少了来自信息处理和分组传输的负载，提高移动网络性能。表 6 从方案的分类、技术方法、应用场景和可扩展性等方面对数据隐私、位置隐私和身份隐私的各类解决方案进行了总结。

6.4 研究方向展望

边缘计算中用户的隐私问题可总结为以下 3 种矛盾。1) 外包数据与数据隐私之间的矛盾；2) 基于位置服务与位置隐私之间的矛盾；3)数据共享与身份隐私保护之间的矛盾。国内外学者为解决这 3 种矛盾展开了深入研究，但所提方案仍然存在很多缺陷，一些可能的研究方向如下。

1) 在保证用户隐私不被泄露的同时支持用户对数据进行各类操作（如审计、搜索和更新等），且各用户之间协同式互操作过程中的隐私问题值得引起广泛关注。

2) 针对基于 TTP 的隐私保护方案在计算能耗上的缺陷，设计轻量级的高效隐私保护方案显得尤为重要。

3) 边缘设备在实际网络中会产生的大量的实时动态数据，这就为攻击者提供了数据关联性、整合分析和隐私挖掘的可能性。因此，从用户的身份、行为、兴趣和位置等角度出发，构建动态和细粒度的数据安全与隐私保护方案是一个重要研究内容。

7 分析与总结

7.1 研究成果总结分析

表 1~表 6 分别从数据保密性、数据完整性、身份认证、访问控制和隐私保护等几个方面概述了现阶段的相应解决方案，各解决方案分别以数据安全与隐私保护研究体系中的一个或几个方面作为研

表 6 现有隐私保护机制分类比较

研究文献	分类	方案	技术方法	应用场景	可扩展性
文献[80]	数据隐私保护	外包云数据的高效隐私保护方案	概率公钥加密系统	云计算	高
文献[81]		轻量级数据隐私保护方案	伪随机置换法	移动多云计算	中等
文献[82]		隐私保护的数据利用技术	可信私有云代理	混合云计算环境	中等
文献[83]	位置隐私保护	基于分布式缓存的位置隐私保护方案	分布式缓存代理	分布式位置服务	高
文献[84]		隐私保护的位置共享系统	基于位置服务	移动在线社交网络	中等
文献[85]		基于缓存感知的虚拟选择算法	位置混淆、隐私度量	位置服务	高
文献[86]		LP-Doctor	位置匿名、信任管理	移动位置应用	中等
文献[87]	身份隐私保护	综合第三方身份管理协议	第三方数字证书管理	移动云计算	中等
文献[88]		基于动态凭证的轻量级身份隐私保护方案	第三方动态凭证管理	移动云计算	高
文献[89]		改进的身份管理协议	完美隐私 PGP 算法	移动互联网应用服务	高

究重点，不断完善各计算范式中的安全机制和协议。其中，值得注意的是，由于边缘计算范式的前瞻性和新颖性，已有研究成果大多集中在除边缘计算以外的其他几种计算范式中，如云计算、移动云计算、雾计算和微云计算等。但这并不意味着对边缘计算的安全性研究需要从零开始。

综上所述，一些适用于其他计算范式的安全机制和组件，很有希望成为边缘计算安全机制的设计基础。例如，移动多云计算环境下的轻量级加密、基于重加密的任务负载分配等方法能为边缘计算中数据保密性和安全计算迁移问题提供解决方案。类似地，跨域身份认证、分级化访问控制以及隐私保护数据挖掘等技术也有望成为边缘计算数据安全与隐私保护机制的有效设计思路。同时，各计算范式之间的差异性应充分考虑，如移动网络运营商基础设施及用户级边缘数据中心的基本特征对安全性的新需求。

7.2　边缘计算相关实例

EdgeX Foundry 框架是由 Linux 基金会发布的一个开源物联网边缘计算项目，它并不是一项边缘计算新标准，而是为了统一标准和边缘应用的一种方式。其目的在于利用可互操作的即插即用部件进而打造出一个物联网开放边缘解决方案[90]。EdgeX Foundry 在构架中定义了“南侧”和“北侧”能力，其中，南侧包括所有的物联网物理设备以及与这些设备、传感器、执行器或者其他对象直接通信的边缘器件；而北侧则是负责数据汇总、存储、聚合、分析和转换的云平台以及负责与云平台通信的网络部分。其基本构架自顶向下分别为输出服务层、支持服务层、核心服务层和设备服务层，这 4 层构架将设备、数据和用户连接起来，并提供独立化、智能化服务。EdgeX Foundry 的主要特性包括：1) 提供灵活的微服务构架；2) 服务具有高扩展性，能够根据设备能力和现实环境进行自由扩展，包括在多个边缘硬件处理器之间进行动态服务分配；3) 以通用 API 的形式支持对移动设备的接口协议转化；4) 在保证高扩展性的同时，具备工业级安全性、稳定性和可靠性。

iFogSim 仿真器是由澳大利亚墨尔本大学 Gupte 等[90]开发的一个采用不同资源管理和调度技术的评估环境，能够实现不同环境和条件下的跨边缘和云资源的应用程序调度策略。在 iFogSim 仿真模型中，传感器将数据发布到物联网络，由边缘云中的应用程序进行处理，得到实时行为信息传递给制动器。其物理实体主要包括 3 个：1) 雾设备，即边缘云设备，用于指定边缘云的硬件特性及接口连接协议；2) 传感器，该实体定义了接入物联网的传感器特征及其输出属性，同时指定连接到该传感器的边缘云的参考属性；3) 执行器，用于指定执行器所连接的网关和定义该连接的网络时延。

OAI 软件平台是欧洲 EURECOM 组织发起并维护的一个开源 SDR LTE 项目，其主要优势在于用软件实现了完整的 3GPP 协议，同时能够结合软件定义无线电组件（SDR）实现 4G LTE 基站。OAI 的实现思想可简单概括为：PC 机通过软件实现物理层和介质访问层功能，同时，实现 3GPP 协议中的各汇聚和控制协议，然后将生成的 IP 数据通过 Linux IP 协议栈进行发送，而此时 eNode B 和 MME 之间通过各自 IP 进行连接和数据交换。目前，OAI 软件平台已经被作为无线电通信技术研究与实现的验证平台。

目前，还有一些其他边缘计算实例（如 JADE[91]、OpenStack[92]等）能够为边缘计算的实现和大规模部署提供验证环境，同时，这些工具和平台也为边缘计算安全和隐私保护方案的实际验证提供解决思路。

8　结束语

本文从边缘计算的基本概念、体系架构和安全问题、数据安全与隐私保护研究体系以及国内外的最新研究成果出发，围绕数据安全、访问控制、身份认证和隐私保护等关键技术，对适用于边缘计算数据安全与隐私保护的最新研究成果进行了阐述和分析。从整体上来说，当前国内外针对边缘计算安全的相关研究和进展还处于初级阶段，尚未形成完整的研究体系，今后的研究工作可侧重于以下 4 个方面。

1) 在面向开放式互联环境的边缘计算中，如何将传统的加密方案与边缘计算中并行分布式架构、终端资源受限和动态性相结合，实现轻量级、分布式的数据安全防护体系是一个亟待解决的问题。

2) 在多信任域共存的边缘计算环境下，应充分考虑信任域与信任实体之间的对应关系，研究不同信任域中各信任实体的身份问题，在实现身份认证的同时兼顾认证功能性和隐私保护特性。

3) 不同信任域之间的多实体访问权限控制。充分考虑边缘计算中跨域、跨群组的分级化访问控制

模式，创建细粒度、动态化和轻量级的多域访问控制机制是非常重要的研究方向。

4) 动态数据安全与细粒度隐私保护。用户在开放互联网环境下会产生大量的实时动态数据，这些数据将会部分或完全在边缘设备中计算处理。而现有的隐私保护方案大多不具有动态防护功能，可扩展性不强。因此，如何在数据动态更新过程中实现细粒度的安全和隐私保护将是一个重大挑战。

只有从上述 4 个方面进行综合考虑，形成完整的安全防护体系，才能有效地保证边缘计算中数据安全和隐私保护的长期演进，从而实现边缘计算服务的健康有序发展。

参考文献：

[1] 施巍松，孙辉，曹杰，等. 边缘计算:万物互联时代新型计算模型[J]. 计算机研究与发展, 2017, 54(5):907-924.
SHI W S, SUN H, CAO J, et al. Edge computing-an emerging computing model for the Internet of everything era [J]. Journal of Computer Research and Development, 2017, 54(5):907-924.

[2] Cisco cloud index supplement. Cloud readiness regional details white paper[R]. 2017.

[3] EVANS D. The Internet of everything: how more relevant and valuable connections will change the world[J]. Cisco IBSG, 2012: 1-9.

[4] LOPEZ P G, MONTRESOR A, EPEMA D, et al. Edge-centric computing: vision and challenges[J]. ACM Sigcomm Computer Communication Review, 2015, 45(5):37-42.

[5] MAO Y Y, YOU C S, ZHANG J, et al. A survey on mobile edge computing: the communication perspective[J]. IEEE Communications Surveys & Tutorials, 2017, PP(99):1.

[6] SHI W S, CAO J, ZHANG Q, et al. Edge computing: vision and challenges[J]. IEEE Internet of Things Journal, 2016, 3(5): 637-646.

[7] ORSINI G, BADE D, LAMERSDORF W. Computing at the mobile edge: designing elastic android applications for computation offloading[C]//The 9th Conference on the Joint IFIP Wireless and Mobile Networking (WMNC'16). 2016:112-119.

[8] DINH H T, LEE C, NIYATO D, et al. A survey of mobile cloud computing: architecture, applications, and approaches[J]. Wireless Communications & Mobile Computing, 2013, 13(18):1587-1611.

[9] BONOMI F, MILITO R, ZHU J, et al. Fog computing and its role in the internet of things[C]//The First Edition of the MCC Workshop on Mobile Cloud Computing. ACM (MCC@SIGCOMM'12). 2012: 13-16.

[10] ABBAS N, ZHANG Y, TAHERKORDI A, et al. Mobile edge computing: a surrey[J]. IEEE Internet of Things Journal, 2017, 5(1): 450-465.

[11] ROMAN R, LOPEZ J, MAMBO M. Mobile edge computing, fog et al.: a survey and analysis of security threats and challenges[J]. Future Generation Computer Systems, 2018, PP(78): 680-698.

[12] SAHAI A, WATERS B. Fuzzy identity-based encryption[C]//The 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT'05). 2005: 457-473.

[13] GOYAL V, PANDEY O, SAHAI A, et al. Attribute-based encryption for fine-grained access control of encrypted data[C]//The 13th ACM Conference on Computer and Communications Security (CCS'06). 2006: 89-98.

[14] WATERS B. Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization[C]//The 14th International Conference on Practice and Theory in Public Key Cryptography (PKC'11). 2011: 53-70.

[15] WANG S L, ZHOU J W, LIU J K, et al. An efficient file hierarchy attribute-based encryption scheme in cloud computing[J]. IEEE Transactions on Information Forensics & Security, 2016, 11(6): 1265-1277.

[16] YANG Y J, LIU J K, LIANG K T, et al. Extended proxy-assisted approach: achieving revocable fine-grained encryption of cloud data[C]//The 20th European Symposium on Research in Computer Security. 2015: 146-166.

[17] ZUO C, SHAO J, WEI G Y, et al. CCA-secure ABE with outsourced decryption for fog computing[J]. Future Generation Computer Systems, 2018, PP(78): 730-738.

[18] BLAZE M, BLEUMER G, STRAUSS M. Divertible protocols and atomic proxy cryptography[C]//The 17th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT'98). 1998: 127-144.

[19] GREEN M, ATENISES G. Identity-based proxy re-encryption[C]//The 5th Applied Cryptography and Network Security (ACNS'07). 2007: 288-306.

[20] WENG J, DENG R H, DING X H, et al. Conditional proxy re-encryption secure against chosen-ciphertext attack[C]//The 4th International Symposium on Information, Computer, and Communications Security (ASIACCS'09). 2009: 322-332.

[21] LIANG K T, MAN H A, LIU J K, et al. A secure and efficient ciphertext-policy attribute-based proxy re-encryption for cloud data sharing[J]. Future Generation Computer Systems, 2015, 52(C): 95-108.

[22] YANG Y J, ZHU H Y, LU H B, et al. Cloud based data sharing with fine-grained proxy re-encryption[J]. Pervasive & Mobile Computing, 2015, 28(C): 122-134.

[23] SHAO J, LU R X, LIN X D, et al. Secure bidirectional proxy re-encryption for cryptographic cloud storage[J]. Pervasive & Mobile Computing, 2016, 28(C): 113-121.

[24] KHAN A N, KIAH M L M, ALI M, et al. A cloud-manager-based re-encryption scheme for mobile users in cloud environment: a hybrid approach[J]. Journal of Grid Computing, 2015, 13(4): 1-25.

[25] KHAN A N, ALI M, KHAN A U R, et al. A comparative study and workload distribution model for re-encryption schemes in a mobile

cloud computing environment[J]. International Journal of Communication Systems, 2017, 30(16): e3308.

[26] RIVEST R L, ADLEMAN L, DERTOUZOS M L. On data banks and privacy homomorphisms[J]. Foundations of Secure Computation, 1978: 169-179.

[27] GENTRY C. Fully homomorphic encryption using ideal lattices[C]// The 41th ACM Symposium on Theory of Computing (STOC'09). 2009: 169-178.

[28] DIJK M V, GENTRY C, HALEVI S, et al. Fully homomorphic encryption over the integers[C]//The 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT'10). 2010: 24-43.

[29] BRAKERSKI Z, VAIKUNTANATHAN V. Efficient fully homomorphic encryption from (standard) LWE[C]//Foundations of Computer Science. 2011: 97-106.

[30] GENTRY C, SAHAI A, WATERS B. Homomorphic encryption from learning with errors: conceptually-simpler, asymptotically-faster, attribute-based[C]//The 33th Annual Cryptology Conference (CRYPTO'13). 2013: 75-92.

[31] LOUK M, LIM H. Homomorphic encryption in mobile multi cloud computing[C]//The 25th International Conference on Information Networking (ICOIN'15). 2015: 493-497.

[32] BAHARON M R, SHI Q, LLEWELLYN-JONES D. A new lightweight homomorphic encryption scheme for mobile cloud computing[C]// 2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing (CIT/IUCC/DASC/PICOM'15). 2015: 618-625.

[33] YANG K, JIA X H. Data storage auditing service in cloud computing: challenges, methods and opportunities[J]. World Wide Web, 2012, 15(4): 409-428.

[34] WANG C, WANG Q, REN K, et al. Privacy-preserving public auditing for data storage security in cloud computing[C]//The 29th IEEE Annual International Conference on Computer Communications (INFOCOM'10). 2010: 1-9.

[35] WANG Q, WANG C, REN K, et al. Enabling public auditability and data dynamics for storage security in cloud computing[J]. IEEE Transactions on Parallel and Distributed Systems, 2011, 22(5): 847-859.

[36] YANG K, JIA X H. An efficient and secure dynamic auditing protocol for data storage in cloud computing[J]. IEEE Transactions on Parallel and Distributed Systems, 2013, 24(9): 1717-1726.

[37] SOOKHAK M, GANI A, KHAN M K, et al. Dynamic remote data auditing for securing big data storage in cloud computing[J]. Information Sciences, 2017, 380(C): 101-116.

[38] LI J T, ZHANG L, LIU J K, et al. Privacy-preserving public auditing protocol for low-performance end devices in cloud[J]. IEEE Transactions on Information Forensics and Security, 2016, 11(11): 2572-2583.

[39] LIN C, SHEN Z D, CHEN Q, et al. A data integrity verification scheme in mobile cloud computing[J]. Journal of Network and Computer Applications, 2017, 77(C): 146-151.

[40] WANG C, CAO N, REN K, et al. Enabling secure and efficient ranked keyword search over outsourced cloud data[J]. IEEE Transactions on Parallel and Distributed Systems, 2012, 23(8): 1467-1479.

[41] CAO N, WANG C, LI M, et al. Privacy-preserving multi-keyword ranked search over encrypted cloud data[J]. IEEE Transactions on parallel and distributed systems, 2014, 25(1): 222-233.

[42] LI H W, LIU D X, DAI Y S, et al. Enabling efficient multi-keyword ranked search over encrypted mobile cloud data through blind storage[J]. IEEE Transactions on Emerging Topics in Computing, 2015, 3(1): 127-138.

[43] LI J, MA R H, GUAN H B. Tees: an efficient search scheme over encrypted data on mobile cloud[J]. IEEE Transactions on Cloud Computing, 2017, 5(1): 126-139.

[44] WANG C J, LI W T, LI Y, et al. A ciphertext-policy attribute-based encryption scheme supporting keyword search function[C]//The 5th International Symposium on Cyberspace Safety and Security (CSS'13). 2013: 377-386.

[45] ZHENG Q J, XU S H, ATENIESE G. VABKS: verifiable attribute-based keyword search over outsourced encrypted data[C]// The 33th Annual IEEE International Conference on Computer Communications (INFOCOM'14). 2014: 522-530.

[46] LIU P L, WANG J F, MA H, et al. Efficient verifiable public key encryption with keyword search based on KP-ABE[C]//The 9th International Conference on Broadband and Wireless Computing, Communication and Applications (BWCCA'14). 2014: 584-589.

[47] SUN W H, YU S C, LOU W J, et al. Protecting your right: verifiable attribute-based keyword search with fine-grained owner-enforced search authorization in the cloud[J]. IEEE Transactions on Parallel and Distributed Systems, 2016, 27(4): 1187-1198.

[48] KAMARA S, PAPAMANTHOU C, ROEDER T. Dynamic searchable symmetric encryption[C]//The 19th ACM Conference on Computer and Communications Security (CCS'12). 2012: 965-976.

[49] KAMARA S, PAPAMANTHOU C. Parallel and dynamic searchable symmetric encryption[C]//The 17th International Conference on Financial Cryptography and Data Security (FC'13). 2013: 258-274.

[50] SUN W H, LIU X F, LOU W J, et al. Catch you if you lie to me: efficient verifiable conjunctive keyword search over large dynamic encrypted cloud data[C]//The 34th Annual IEEE International Conference on Computer Communications (INFOCOM'15). 2015: 2110-2118.

[51] XIA Z H, WANG X H, SUN X M, et al. A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data[J]. IEEE Transactions on Parallel and Distributed Systems, 2016, 27(2): 340-352.

[52] HU B S, LIU Q, LIU X H, et al. DABKS: dynamic attribute-based keyword search in cloud computing[C]//2017 IEEE International

Conference on Communications (ICC'17). 2017: 1-6.

[53] SHAO J, CAO Z F, LIANG X H, et al. Proxy re-encryption with keyword search[J]. Information Sciences, 2010, 180(13): 2576-2587.

[54] WANG X A, HUANG X Y, YANG X Y, et al. Further observation on proxy re-encryption with keyword search[J]. Journal of Systems and Software, 2012, 85(3): 643-654.

[55] FANG L M, SUSILO W, GE C P, et al. Chosen-ciphertext secure anonymous conditional proxy re-encryption with keyword search[J]. Theoretical Computer Science, 2012, 462: 39-58.

[56] SHI Y F, LIU J Q, HAN Z, et al. Attribute-based proxy re-encryption with keyword search[J]. PloS One, 2014, 9(12): e116325.

[57] LIU H, NING H S, XIONG Q X, et al. Shared authority based privacy-preserving authentication protocol in cloud computing[J]. IEEE Transactions on Parallel and Distributed Systems, 2015, 26(1): 241-251.

[58] TSAI J L, LO N W. A privacy-aware authentication scheme for distributed mobile cloud computing services[J]. IEEE Systems Journal, 2015, 9(3): 805-815.

[59] JIANG Q, MA J F, WEI F S. On the security of a privacy-aware authentication scheme for distributed mobile cloud computing services[J]. IEEE Systems Journal, 2017, PP(99): 1-4.

[60] HE D B, KUMAR N, KHAN M K, et al. Efficient privacy-aware authentication scheme for mobile cloud computing services[J]. IEEE Systems Journal, 2017, PP(99): 1-11.

[61] LO N W, TSAI J L. An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks without pairings[J]. IEEE Transactions on Intelligent Transportation Systems, 2016, 17(5): 1319-1328.

[62] MAHMOOD K, CHAUDHRY S A, NAQVI H, et al. An elliptic curve cryptography based lightweight authentication scheme for smart grid communication[J]. Future Generation Computer Systems, 2017, PP(81): 557-565.

[63] TOOSI A N, CALHEIROS R N, BUYYA R. Interconnected cloud computing environments: challenges, taxonomy, and survey[J]. ACM Computing Surveys (CSUR), 2014, 47(1): 7.

[64] TOUCEDA D S, CAMARA J M S, ZEADALLY S, et al. Attribute-based authorization for structured peer-to-peer (P2P) networks[J]. Computer Standards & Interfaces, 2015, 42(C): 71-83.

[65] YANG Y, ZHENG X H, LIU X M, et al. Cross-domain dynamic anonymous authenticated group key management with symptom-matching for e-health social system[J]. Future Generation Computer Systems, 2017, PP(99): 1-7.

[66] YANG X, HUANG X Y, LIU J K. Efficient handover authentication with user anonymity and untraceability for mobile cloud computing[J]. Future Generation Computer Systems, 2016, 62(C): 190-195.

[67] MCCARTHY D, MALONE P, HANGE J, et al. Personal cloudlets: implementing a user-centric datastore with privacy aware access control for cloud-based data platforms[C]//The First International Workshop on TEchnical and LEgal aspects of data pRIvacy. 2015: 38-43.

[68] HE D B, ZEADALLY S, WU L B, et al. Analysis of handover authentication protocols for mobile wireless networks using identity-based public key cryptography[J]. Computer Networks, 2017, PP(28): 154-163.

[69] YU S C, WANG C, REN K, et al. Achieving secure, scalable, and fine-grained data access control in cloud computing[C]//The 29th Annual IEEE International Conference on Computer Communications (INFOCOM'10). 2010: 1-9.

[70] XUE K P, XUE Y J, HONG J N, et al. RAAC: robust and auditable access control with multiple attribute authorities for public cloud storage[J]. IEEE Transactions on Information Forensics and Security, 2017, 12(4): 953-967.

[71] JIN Y, TIAN C, HE H, et al. A secure and lightweight data access control scheme for mobile cloud computing[C]//The 5th International Conference on Big Data and Cloud Computing (BDCloud'15). 2015: 172-179.

[72] ZHANG P, CHEN Z H, LIU J K, et al. An efficient access control scheme with outsourcing capability and attribute update for fog computing[J]. Future Generation Computer Systems, 2018, PP(78): 753-762.

[73] HUANG Q L, YANG Y X, WANG L C. secure data access control with ciphertext update and computation outsourcing in fog computing for internet of things[J]. IEEE Access, 2017, 5(99):12941-12950.

[74] ZHOU L, VARADHARAJAN V, HITCHENS M. Achieving secure role-based access control on encrypted data in cloud storage[J]. IEEE Transactions on Information Forensics and Security, 2013, 8(12): 1947-1960.

[75] CHEN H C. A hierarchical virtual role assignment for negotiation-based RBAC scheme[C]//The 10th International Conference on Broadband and Wireless Computing, Communication and Applications (BWCCA'15). 2015: 538-543.

[76] KUHN D R, COYNE E J, WEIL T R. Adding attributes to role-based access control[J]. Computer, 2010, 43(6): 79-81.

[77] LI H J, WANG S, TIAN X X, et al. A survey of extended role-based access control in cloud computing[C]//The 4th International Conference on Computer Engineering and Networks (CENeT'14). 2015: 821-831.

[78] ALMUTAIRI A, SARFRAZ M, BASALAMAH S, et al. A distributed access control architecture for cloud computing[J]. IEEE Software, 2012, 29(2): 36-44.

[79] CHEN L Q, URIAN R. DAA-A: direct anonymous attestation with attributes[C]//The 8th International Conference on Trust and Trustworthy Computing (TRUST'15). 2015: 228-245.

[80] PASUOULETI S K, RAMALINGAM S, BUYYA R. An efficient and secure privacy-preserving approach for outsourced data of resource constrained mobile devices in cloud computing[J]. Journal of Network and Computer Applications, 2016, 64(C): 12-22.

[81] BAHRAMI M, SINGHAL M. A light-weight permutation based method for data privacy in mobile cloud computing[C]//The 3th International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud'15). 2015: 189-198.

[82] LI J W, LI J, CHEN X F, et al. Privacy-preserving data utilization in hybrid clouds[J]. Future Generation Computer Systems, 2014, 30(1): 98-106.

[83] CHEN M, LI W Z, LI Z, et al. Preserving location privacy based on distributed cache pushing[C]//2014 IEEE Wireless Communications and Networking Conference (WCNC'14). 2014: 3456-3461.

[84] WEI W, XU F Y, LI Q. Mobishare: flexible privacy-preserving location sharing in mobile online social networks[C]//The 31th Annual IEEE International Conference on Computer Communications (INFOCOM'12). 2012: 2616-2620.

[85] NIU B, LI Q H, ZHU X Y, et al. Enhancing privacy through caching in location-based services[C]//The 34th Annual IEEE International Conference on Computer Communications (INFOCOM'15). 2015: 1017-1025.

[86] FAWAZ K, HUAN F, SHIN K G. Anatomization and protection of mobile apps' location privacy threats[C]//The 24th USENIX Conference on Security Symposium (USENIX SEC'15). 2015: 753-768.

[87] KHALIL I, KHREISHAH A, AZEEM M. Consolidated identity management system for secure mobile cloud computing[J]. Computer Networks, 2014, 65(2):99-110.

[88] KHAN A N, KIAH M L M, MADANI S A, et al. Enhanced dynamic credential generation scheme for protection of user identity in mobile-cloud computing[J]. The Journal of Supercomputing, 2013, 66(3): 1687-1706.

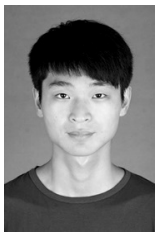
[89] PARK I S, LEE Y D, JEONG J. Improved identity management protocol for secure mobile cloud computing[C]//The 46th Hawaii International Conference on System Sciences (HICSS'13). 2013: 4958-4965.

[90] GUPTA H, DASTJERDI A V, GHOSH S K, et al. iFogSim: a toolkit for modeling and simulation of resource management techniques in internet of things, edge and fog computing environments[J]. Software Practice & Experience, 2017, 47(9): 1275-1296.

[91] BELLIFEMINE F L, CAIRE G, Greenwood D. Developing multi-agent systems with JADE[M]. New York: John Wiley & Sons, 2007.

[92] ROSADO T, BERNARDINO J. An overview of openstack architecture[C]//The 18th International Database Engineering & Applications Symposium (IDEAS'14). 2014: 366-367.

[作者简介]



张佳乐（1994-），男，安徽蚌埠人，南京航空航天大学博士生，主要研究方向为边缘计算、数据安全和应用密码学。

赵彦超（1985-），男，江苏连云港人，南京航空航天大学副教授，主要研究方向为计算机网络、智能感知计算、无线网络、感知数据处理等。

陈兵（1970-），男，江苏南通人，南京航空航天大学教授、博士生导师，主要研究方向为计算机网络、认知无线电、无线通信、下一代网络及信息安全等。

胡峰（1987-），男，江苏扬州人，南京航空航天大学博士生，主要研究方向为无线网络、移动网络和认知无线电。

朱琨（1984-），男，安徽合肥人，南京航空航天大学教授、博士生导师，主要研究方向为下一代无线通信网络（5G）、自组织网络、D2D 通信及无线虚拟化技术等。