DOI:10.7544/issn1000-1239.20210644
59(4):765-780,2022

边缘计算环境下安全协议综述

李晓伟[1] 陈本辉[1] 杨邓奇[1] 伍高飞[2,3]
[1](大理大学数学与计算机学院 云南大理 671003)
[2](广西密码学与信息安全重点实验室(桂林电子科技大学) 广西桂林 541000)
[3](西安电子科技大学网络空间安全学院 西安 710071)
(lixiaowei_xidian@163.com)

Review of Security Protocols in Edge Computing Environments

Li Xiaowei[1], Chen Benhui[1], Yang Dengqi[1], and Wu Gaofei[2,3]
[1](*College of Mathematics and Computer Science, Dali University, Dali, Yunnan* 671003)
[2](*Guangxi Key Laboratory of Cryptography and Information Security (Guilin University of Electronic Technology), Guilin, Guangxi* 541000)
[3](*College of Cyberspace Security, Xidian University, Xi'an* 710071)

Abstract The rapid popularity of the Internet of things has caused the scale of data to rise geometrically. The method of processing data concentrated in the cloud center gradually has problems such as communication delay and privacy leakage. Edge computing sinks part of the cloud center business to the edge of the device enabling data processing to be completed on the terminal network, thereby achieving rapid data processing. At the same time, as long-distance communication is avoided, user data can be transferred locally, so that user privacy data can be safely protected. However, the change of network architecture puts forward new requirements for security protocols in the edge computing environment. The classification and summary of security protocols in the edge computing environment is helpful to relevant practitioners quickly grasp the research progress in this field, and it will also help beginners in the field of edge computing security to quickly understand the application methods of security protocols in this field. The typical research results of authentication protocols, key agreement protocols, privacy-preserving protocols, and data sharing protocols in the edge computing environment are reviewed, and each kind of security protocols is specifically classified, analyzed and summarized. The core problems of security protocols in the edge computing environment are given, and specific research directions and suggestions are given for each protocol field. The purpose of overall grasp of the research progress of security protocols in the current edge computing environment is achieved.

Key words edge computing; security protocol; authentication and key agreement; privacy-preserving; data sharing

收稿日期:2021-06-11;**修回日期**:2021-09-24

基金项目:国家自然科学基金项目(61902049,31960119,51809026);云南省科技厅项目(2018FH001-062,2018FH001-063);广西密码学与信息安全重点实验室研究课题(GCIS202123);大理大学创新团队项目(ZKLX2020308)
This work was supported by the National Natural Science Foundation of China (61902049, 31960119, 51809026), the Project of Yunnan Provincial Department of Science and Technology (2018FH001-062, 2018FH001-063), the Project of Guangxi Key Laboratory of Cryptography and Information Security (GCIS202123), and the Project of Dali University Innovation Team (ZKLX2020308).

通信作者:伍高飞(wugf@nipc.org.cn)

摘 要 物联网的迅速普及使得数据规模以几何式上升.集中在云中心处理数据的方式逐渐出现通信时延及隐私泄露等问题.边缘计算将部分云中心业务下沉到设备边缘,使得数据处理在终端网络完成,从而实现数据快速处理.同时,由于避免了远距离通信,用户数据在本地处理,使得用户隐私数据得以安全保护.然而网络架构的改变对边缘计算环境下的安全协议又提出了新的要求.对边缘计算环境下安全协议进行分类总结有助于相关从业人员快速掌握该领域的研究进展,更有助于边缘计算安全领域的初学者快速了解安全协议在该领域中的应用方法.综述了近年来边缘计算环境下认证协议、密钥协商协议、隐私保护协议以及数据共享协议的典型研究成果,对每个安全协议进行了具体的分类、分析及总结.给出了边缘计算环境下安全协议所存在的核心问题并针对这些问题给出了具体的研究方向及建议.实现了对边缘计算环境下安全协议研究进展进行总体把握的目的.

关键词 边缘计算;安全协议;认证与密钥协商;隐私保护;数据共享

中图法分类号 TP309

物联网的快速发展和应用使得终端数据呈现海量增长趋势.数据集中传输到云端处理的方式逐渐产生弊端.一方面这样的方式不能满足需要快速实时处理数据的应用场景,如当出现紧急事故时应该立即启动应急响应措施,而不是再经过云中心处理;另一方面对于涉及用户隐私的数据传输到云中心处理会存在隐私泄露的风险,如摄像头采集的用户图像数据必须传输到云中心才能处理则有可能泄露用户隐私.

边缘计算从某种程度上解决了上述问题[1].边缘计算是指数据的计算、存储以及应用可以在数据源头的网络边缘处完成,而无需传输到云中心.边缘计算大大减轻了云中心数据处理以及网络传输瓶颈.在设备边缘处理用户隐私数据也避免了泄露[2].更为重要的是当安全事故发生时可以使应急响应迅速执行.在物联网设备日渐趋于泛化的情况下,边缘计算所带来的云—边协同效应必将推动物联网行业快速变革.根据 Grand View Research 的最新报告,到 2027 年,全球边缘计算市场规模预计将达到 154 亿美元,预测期内复合年增长率为 38.6%[3].

边缘计算环境下计算、存储以及数据传输具有较强的分布式特点,其业务协同需要安全支撑.然而失去云中心强大的安全保障,在设备边缘进行的数据存储、传输以及应用受到巨大的安全挑战.网络安全协议可以解决边缘计算中的上述安全问题。而随着网络架构从云—端转变到云—边—端甚至边—端,如何设计符合边缘计算的网络安全协议是边缘计算发展过程中所必须要解决的问题.

本文首先给出安全协议概念、边缘计算环境下通信的特点及安全风险分析,然后综述了近年来边缘计算环境下认证、密钥协商、隐私保护以及数据共享 4 类安全协议的最新进展,最后给出了边缘计算环境下安全协议存在的问题以及研究方向建议.

本文尝试以简单的形式给出近年来边缘计算环境下安全协议研究进展.一方面以期实现对目前边缘计算环境下安全协议研究进展进行总体把握的目的;另一方面通过对安全协议的表述、边缘计算通信特点及风险的概括以期实现对边缘计算尤其是其安全协议实现科普的目的.

1 安全协议及边缘计算概述

1.1 安全协议概述

安全协议是网络通信中为实现某种安全目的,通信双方或多方按照一定规则采用密码学技术完成的一系列消息交互的过程.安全协议是网络通信安全的基础,是网络通信安全首先要考虑的问题.一般而言,安全协议按照功能不同主要分为认证协议、密钥协商协议、隐私保护协议以及数据共享协议 4 类协议,4 类协议之间相互协同共同实现网络通信安全.4 类协议的概述为:

1) 认证协议(Authentication Protocol).认证是指在网络环境下证明实体拥有其声称的实体身份或证明发送的消息真实性,其包括身份认证和消息认证.身份认证一般通过验证用户拥有的秘密凭证如口令等来实现.消息认证一般通过数字签名以及消息认证码来实现.

2) 密钥协商协议(Key Exchange Protocol).密钥协商是指通信双方或多方借助密码学手段实现密钥共享,以此建立消息保密、消息完整性等安全需求所需的密钥.密钥协商一般分为对称密钥协商以及非对称密钥协商.

3) 隐私保护协议(Privacy-preserving Protocol).隐私保护是指通信过程中或者业务流程中用户的个人隐私不会被泄露.用户隐私一般包括用户数据隐私、位置隐私、身份隐私等.隐私保护可以通过传统密码学方式来实现,如加密处理等,也可以采用非密码方式如差分隐私的方式来实现.

4) 数据共享协议(Data Sharing Protocol).数据共享是指数据可以被授权的实体所安全的访问、使用,数据共享权利不被非法地篡改或者剥夺.数据共享除使用传统访问控制实现外,更多的是通过密码学方式实现,如可以通过属性加密、代理重加密等方法实现.

1.2 边缘计算通信特点

边缘计算解决物联网设备和云中心之间的通信效率、计算效率以及应用服务扩展等问题.其功能主要是通过边缘计算节点来实现的.边缘计算节点部署在物联网终端和云服务商之间,可以看成是终端和云之间的中间组件.边缘计算环境下的通信具体涉及终端设备和边缘节点之间通信、边缘节点和云中心之间通信以及终端设备和终端设备之间的通信,其往往具有5个特点:

1) 终端设备数量巨大.物联网设备规模目前已达到百亿级,随着边缘计算应用的不断增加,物联网边缘终端设备数量仍将快速增长.

2) 终端设备性能受限.虽然随着计算及存储技术的提升,物联网设备已经具有一定的通信及计算能力,但总体来讲其性能仍有待提升.仅少部分终端可以具备较高的通信能力及计算能力.

3) 边缘设备需快速响应.与传统的物联网相比,边缘计算的优点是更加及时地处理终端数据,其更加关注数据处理的效率.

4) 设备来自不同异构网络,形成不同信任域.边缘计算节点往往将部署在其边缘的设备划分成一个可信域.该节点无法具有骨干网中服务器节点的覆盖范围,因此边缘计算环境下通信往往会涉及到不同域间通信,即边缘节点覆盖下的跨域间的终端通信.

5) 频繁的数据共享.在设备边缘处理数据使得数据不必传输到云中心,这为数据在设备边缘的快速共享提供可能,基于边缘节点的数据共享应用将大量出现.

边缘计算下通信虽然具有物联网的基本特点,但也呈现出一些关键的区别,如边缘计算节点划分的跨域间通信以及频繁的数据共享等.因此,边缘计算环境下的通信需要新的安全协议来支撑.

1.3 边缘计算通信安全风险分析

边缘计算从云中心网络架构中衍生出来不可避免地具有普通云环境中的通信安全风险.同时,由于边缘计算呈现分布式安全域且其通信主体更容易被攻陷(如边缘节点、终端设备往往部署在用户端,无法提供更强的安全保护),因此边缘计算又有其自身的通信安全风险.具体而言,边缘计算通信存在4个安全风险:

1) 认证授权风险.边缘计算网络架构中通信主体无论是边缘节点还是终端设备往往部署在用户端,从而起到快速数据收集及数据传输的目的.而用户端的设备相比云中心更容易被窃取、中间人攻击、假冒以及攻陷等攻击,这就给边缘计算终端设备认证及授权提出了巨大的挑战.同时,由于其自身的性能受限,不可能在其上部署较强的安全方案,进一步对边缘计算认证协议提出了更高的要求.

2) 基础设施及用户设备安全风险.一方面边缘计算基础设施容易遭受拒绝服务攻击、窃听、无线干扰等威胁.例如攻击者可以伪造网关等基础设施,从而完成窃听等攻击.另一方面终端用户可能有意或者无意(被控制)地向其他设备传播恶意代码.由于用户设备间往往组成一个信任域,域内设备往往是可信的,这样导致一个设备被攻陷其他设备可能都将被攻陷.同时,数据大都存储在终端或者边缘节点,这样的方式数据更容易被攻击者损坏或者伪造.而没有云中心的备份,一旦数据丢失较难恢复.

3) 分布式多安全域间通信风险.边缘计算节点将终端设备分成多个安全域,域与域之间往往需要协同工作.不同安全域间存在设备窃听、假冒、中间人攻击等风险.同时,由于不同安全域往往部署的安全凭证不同,域与域之间要建立安全通道也较为复杂.另一方面异构网络间通信中面临网络切换,在快速通信切换过程中也面临异构网络通信认证及授权等问题.

4) 隐私泄露风险.边缘计算处理数据流程一般为终端将数据上传到边缘节点,边缘节点处理后(自身处理或和云中心协同处理)又将数据返回到终端.虽然边缘计算数据不再由用户直接远距离传输给云中心,避免了远距离通信带来的隐私泄露风险.但是边缘计算通信中仍然涉及用户上传边缘节点数据隐私、边缘节点发送给终端数据隐私.同时还涉及边缘节点在处理用户数据时的计算隐私,即边缘节点在处理用户数据时会不会泄露用户数据.缺乏云中心

强大的隐私保护措施,边缘节点将面临多目标、多途径、多形式的隐私泄露威胁.

2 边缘计算环境下安全协议进展

由于边缘计算环境下通信存在诸多安全风险,其需要新的适用于边缘计算环境下的安全协议来支撑.本文不一一列举边缘计算安全协议的研究成果,而是在这些成果中选取近几年一些有代表性的成果进行分类总结(2018 年以来成果),以期达到从总体上把握边缘计算安全协议最新研究进展的目的,为相关行业从业人员和科研人员快速掌握边缘计算安全协议研究现状提供帮助.

2.1 边缘计算环境下认证协议

认证协议是网络安全通信所需要进行的基本协议.按照不同的认证结构,本文将边缘计算环境下认证划分为:固定边缘计算节点认证、非固定边缘计算节点认证以及分布式跨域认证.

1) 固定边缘计算节点认证.边缘计算的引入使得原本云—端的网络架构变为云—边—端的 3 层网络架构,因此认证模式也将随之改变.终端要获得边缘服务器节点的服务,彼此之间首先要进行认证.固定边缘计算节点认证是在物联网中把性能相对较好的设备或者实体作为边缘计算节点,这个节点一直充当边缘计算节点的作用.固定边缘计算节点认证协议如表 1 所示:

Table 1 Fixed Edge Computing Node Authentication Protocols in Edge Computing Environments

表 1 边缘计算环境下固定边缘计算节点认证协议

方案	解决问题	技术方法(模式)	优劣势
车载网络环境下安全雾计算服务切换的双向认证方案[4]	云—边—端构下的认证	云中心发放凭证后充当边—端的辅助来完成第三方认证	较为直观便捷的认证方式,但没有从本质上解决云中心为认证核心的模式.
移动边缘计算下可证明安全的无需可信中心的基于动态身份的认证密钥协议[5]	边—端架构下的认证	依据认证中心发放签名凭证作为各方认证凭证	云中心做离线处理,避免了云中心实时处理大量认证请求的问题.
基于身份的移动边缘计算匿名身份验证方案[6]	边—端架构下的认证	依据认证中心发放签名凭证作为各方认证凭证	具有隐私保护功能,使用双线性对不适用低性能物联网设备.
移动边缘计算下基于身份的具有匿名属性的认证方案[7]	云—边—端构下的认证	依据认证中心发放签名凭证作为各方认证凭证	利用云中心作为辅助完成边缘节点和终端的认证,方法简单
智能车联网可扩展且有效的匿名批量认证方案[8]	批量认证	依据认证中心发放的具有聚合性质的签名凭证实现	具有隐私保护功能,采用批量认证效率较高.
基于代理的云边缘联合身份验证方案[9]	联合认证	EAP-AKA 的认证框架	联合认证减轻用户频繁认证负担,需要有一个可信第三方作为联合认证中心.

在这种模式下进行认证,一种直观的方式就是终端和边缘计算节点都在云中心注册,云中心充当边缘服务器节点和终端设备的可信模块协助完成认证.Dewanta 等人[4]考虑的即是这种模式.终端设备(如手机、车辆等)如要接收边缘服务器节点的服务,先是提交认证请求到云中心,在云中心的协助下完成终端和边缘计算节点(如网关或者车联网中的路边单元)的相互认证.这样的方式相对便捷,同时认证凭证存储在云中心有一定的安全性.但这样的方式仍没有改变云中心要处理大量认证请求的问题,所有信息依然需要云中心处理.Mishra 等人[5]及 Jia 等人[6]分别提出边—端的认证方式,即认证过程只有边缘计算节点和终端,其本质相当于将云中心做离线处理.终端在和边缘计算节点认证前分别在云中心注册,获取凭证(类似于一个对身份的签名),然后通过交换认证凭证完成认证.该方法避免了云中心实时处理大量认证请求的问题.Li 等人[7]将身份隐私引入到上述类似架构中,基于身份密码学提出具有隐私保护的边缘认证方案.Zhang 等人[8]提出具有批量认证功能的智能车联网认证方案,其本质也是路边单元(road side unit, RSU)在收到终端的批量认证请求时利用云中心颁发给终端的签名凭证完成批量认证.在云—边—端的网络架构中,终端设备既要与云中心认证又要与边缘服务器认证,考虑到这一点,Lin 等人[9]提出基于代理的云边联合认证方案,即由一个可信第三方协助完成各设备的认证.采用类似 EAP-AKA(extensible authentication protocol-authentication and key agreement)的认证框架,给出了低认证时延的方案.

2) 非固定边缘计算节点认证.非固定边缘计算节点是指在边缘计算环境中选取的边缘计算节点可

以失去其边缘计算的作用,而其他之前没有作为边缘节点的设备可能被视为新的边缘计算节点.这样的架构中边缘节点更加灵活,更能适应复杂的认证环境.具体方案如表 2 所示:

Table 2 Unfixed Edge Computing Node Authentication Protocols in Edge Computing Environments

表 2 边缘计算环境下不固定边缘计算节点认证协议

方案	解决问题	技术方法(模式)	优劣势
基于边缘计算的车载自组网高效消息认证方案[10]	非固定边缘节点认证	将性能好的车辆作为临时边缘节点再通过签名凭证进行认证	边缘节点不固定,避免固定边缘节点遭受的单点攻击.
边缘计算下支持 5G 的车载网络隐私保护身份认证协议[11]	5G 场景下非固定边缘节点认证	通过签名凭证进行认证	支持 5G 场景通信,具有隐私保护属性,支持群组认证.
车辆边缘计算中具有数据可追溯性的区块链协作认证[12]	分布式边缘节点认证	认证过程卸载给其他多个节点	通过秘密分割方式完成分布式认证,认证方式更为灵活.未考虑秘密共享者变动的情况.
基于边缘计算的车联网多设备消息认证方案[13]	手机作为边缘节点认证	环签名进行认证	新颖的认证方式,将手机作为边缘计算节点,但采用环签名方式完成认证过程相对复杂.
基于移动边缘计算的切换认证方案[14]	移动边缘节点跨域认证	参与实体间共享密钥认证	移动边缘网络场景,支持漫游认证.采用对称的方式完成,通信多方必须提前共享密钥凭证.

Cui 等人[10]首先提出非固定边缘计算节点的认证方案.考虑车联网场景,将车辆分为边缘计算车辆(edge computing vehicles, ECV)以及普通车辆(ordinary vehicles, OV),由性能较高的车辆动态地作为边缘计算节点完成高效认证.认证过程是通过颁发基于身份的签名作为认证凭证.其方案的显著特点是在批量认证的同时基于布谷过滤器消除重复认证提高批量认证效率.Zhang 等人[11]提出了边缘计算环境中基于 5G 的车联网认证与密钥协商协议.认证过程中不再由路边单元 RSU 提供认证服务,而是由动态形成的车辆作为边缘计算节点,由边缘计算节点来完成认证.通过采用云中心的签名凭证作为认证凭证实现批量认证.为避免单一边缘认证中心节点负担过重从而减轻边缘计算节点的计算压力,Liu 等人[12]提出基于秘密共享的分布式认证,通过秘密共享的方式将认证过程卸载给多个边缘设备.在 RSU 附近产生代理车辆节点用来辅助认证.RSU 将秘密通过拉格朗日差值多项式分布成 n 个份额,分发给 n 个车辆,车辆中有 k 个认证通过才能完成认证($k \leqslant n$).以往大多数边缘计算认证方案中都是将基站或者车辆网中的路边设施单元 RSU 作为边缘计算节点.Zhong 等人[13]考虑到在某些通信场景中,和相对性能较弱的终端设备比较,手机可以看作边缘计算节点,实现计算任务卸载到手机上从而保证快速灵活认证.该思想为边缘计算下认证提供了一种新的方法,但是其认证过程稍显复杂.其采用的是通过手机端实现环签名,其他终端通过验证环签名实现认证.Wang 等人[14]考虑当移动设备作为边缘计算节点时,其需要从一个接入点(access point, AP)范围离开进入另一个 AP 范围时的认证问题.文献[14]提出的认证方案使用的方法是通过每个参与实体间共享对称密钥完成认证.

3) 边缘计算分布式跨域认证.总结而言,已有的跨域认证协议大致可以分为 2 类:①基于一个可信中心作为中间点,如云中心,由云中心为 2 个不同实体传递认证凭证从而达成认证共识.这样的方式相对简单,但需要可信中心实时参与运行.②不需要可信中心参与,终端或者边缘节点在云中心注册得到认证凭证后,通过认证凭证自行跨域认证.这样的方式避免了可信中心因大量通信及计算消耗导致的时延,但往往终端之间需要额外的计算.具体方案如表 3 所示.

Dewanta 等人[4]提出了边缘计算环境下基于云中心的跨域认证协议可以看成是第 1 类跨域认证协议.其方法是用户在云中心注册后得到一个对称密钥形成的认证凭证,然后由云中心把相应的凭证再发给其他边缘计算节点,其他节点用已有的对称凭证对终端进行认证.Wang 等人[15]的方案可以看出是第 2 类跨域认证.Wang 等人[15]提出终端设备组成群组情况下的无中心认证.不同群组分配群公私钥,通过类似群签名的方式完成不同群成员之间的认证.类似的跨域方案还有 He 等人[16]提出的移动医疗网络环境下跨域方案.文献[16]对跨域下认证方案给出了详细的安全证明,为跨域认证提供了更

多理论支撑.分布式跨域认证需要一种分布式的技术作为支撑.区块链具有去中心化、分布式、不易篡改、可追溯等特点,适合于分布式可信平台的认证需求.基于此,Zhang 等人[17]考虑移动边缘计算环境中设备认证与区块链结合.将认证中心颁发的临时公钥存于区块链中实现跨域批量认证.由于区块链具有不可篡改的特点,因此将临时公钥部署到区块链上变相地实现了对临时公钥认证的目的.Guo 等人[18]采用类似的方法,将公钥放到区块链中实现有效性证明,同时将用户登录过程写入智能合约,从而完成交易确认.跨域场景往往使用公钥密码作为底层认证技术,而使用公钥证书时验证证书撤销列表是非常耗时的,结合区块链技术对证书进行验证可以解决这个问题.Wang 等人[19]提出将公钥放到区块链中,通过验证区块链数据的有效性从而验证公钥的有效性,避免查看证书吊销列表.但是该方案没讨论引入区块链进行验证是否同样会引发同证书撤销列表同样的时间消耗.

Table 3 Distributed Cross-domain Authentication Protocols in Edge Computing Environments

表 3 边缘计算环境下分布式跨域认证协议

方案	解决问题	技术方法(模式)	优劣势
车载网络环境下安全雾计算服务切换的双向认证方案[4]	有可信中心的跨域认证	云中心发放凭证后充当边—端的辅助来完成认证	任何认证都许经过中心节点,这样的认证方式最为简单,但需要中心实时参与.
边缘计算环境下无中心的分散式认证[15] 移动医疗社交网络的可证明安全的跨域握手方案[16]	无可信中心的跨域认证	通过对身份的签名凭证完成无中心认证	2 种方案都属于无中心跨域认证,文献[15]采用群签名方式完成跨域认证,方案略显复杂.文献[16]仅采用高效的签名凭证完成跨域认证.
基于区块链的移动边缘计算的群签名和认证方案[17]	边缘计算环境中公钥证书真伪验证问题	将证书信息写入区块链	证书写入区块链,证书真伪的验证无需证书中心.没有考虑证书撤销的验证.
区块链与边缘计算结合的分布式可信认证方案[18]	公钥证书验证以及登录过程确认问题	将登录验证过程以智能合约形式写入区块链	进一步将用户登录过程写入区块链,使得用户无法抵赖.
基于区块链的智能电网环境下匿名身份验证[19]	公钥证书撤销验证问题	将证书信息写入区块链	将证书是否撤销验证放入区块链中,避免了长时间查询证书撤销列表.但方案没讨论引入区块链进行验证是否同样会引发同证书撤销列表同样的时间消耗.

4) 边缘计算认证协议总结.已有边缘计算认证协议基本解决了认证协议中的安全问题,同时考虑了多种场景下的认证协议,如非固定边缘节点认证、手机等移动设备作为边缘节点认证以及跨域认证等.但边缘计算认证协议仍没有从本质上改变云中心作为认证核心的架构,仍大都采用云中心分发凭证的模式.这样的模式仍然会造成单点失效以及通信时延等问题.虽然有灵活的边缘计算节点如车辆手机等作为认证过程中媒介,但从分布式认证角度来看仍没有完全脱离中心认证.同时,边缘计算本身具有多信任域的特征,需要跨域认证协议作为支撑.虽然有一些跨域认证协议被提出,但目前仍没有非常完善的边缘计算环境下的跨域认证协议.区块链作为解决分布式问题的技术已有用来解决边缘计算分布式认证问题,但大都是在分布式认证过程中的证书鉴别过程使用区块链,即通过将证书上链来简化证书鉴别从而实现身份鉴别.目前仍需要探索更多方式的区块链应用来解决边缘计算认证问题.

2.2 边缘计算环境下密钥协商协议

认证与密钥协商往往是不可分割的部分,即认证后往往需要协商一个共享的密钥后才能进行安全通信.已有的边缘计算环境下密钥协商协议从本质上来说大致可以分为基于对称密码体制的密钥协商和基于非对称密码体制的密钥协商 2 类,具体如表 4 所示.

1) 非对称密钥协商.这里不一一列举边缘计算环境下非对称密钥协商协议,而是总结非对称密钥协商协议本质特征,给出通用的实现方法.非对称密钥协商也就是双方采用公钥的方式完成密钥协商.典型方案有 Jia 等人[6]的方案,Zhang 等人[11]的方案以及 Wang 等人[19]的方案.其核心是终端节点在云中心或者边缘节点注册,云中心或边缘节点会颁发一个 ElGamal 签名凭证给终端,终端通过该签名凭证完成密钥协商.具体过程为:设在椭圆曲线密码体制下(具体参数略),终端设备 V_i 的身份信息为 ID_{V_i},其向服务器 S 提出注册请求后,服务器选择一个随机数 $r_{V_i}\in\mathbb{Z}_q^*$ 并计算 $R_i=r_iP$, $h_i=H(ID_{V_i}\|R_i)$.服务器 S 利用自己的私钥 s(对应公钥为 sP)计算出 V_i 的凭证 $s_{V_i}=r_i+h_i\times s$.本质上相当于颁发一个没有证书的公钥给终端,终端收到该凭证后再利用

Diffie-Hellman 密钥协商算法完成密钥协商(具体见文献[6]).这样的方式最为直观,但每次验证时都需要服务器公钥参与运行.由于边缘环境下存在多个不同的域,也就意味着进行密钥协商时需要验证多个边缘服务器的公钥,而这又涉及繁琐的数字证书管理问题.

Table 4 Key Agreement Protocols in Edge Computing Environments

表 4 边缘计算环境下密钥协商协议

分类	方案	解决问题	技术方法(模式)	优劣势
非对称密钥协商	基于身份的移动边缘计算匿名身份认证方案[6]	无中心环境下终端与边缘节点密钥协商	利用认证中心颁发的对身份的签名作为临时公钥,再结合 Diffie-Hellman 密钥协商协议思想进行密钥协商	详细的安全性证明,但方案采用双线性对运算,不适用于低性能物联网设备.
	边缘计算下支持 5G 的车载网络的隐私保护身份认证协议[11]	非固定边缘节点密钥协商		支持群组密钥协商,具有隐私保护功能.
	基于边缘计算的智能电网多设备消息认证方案[19]	多设备密钥协商	利用区块链,将认证用户更新和撤销写入智能合约	考虑了成员变动的场景,没有形式化的证明.
对称密钥协商	一种轻量级的匿名双向身份验证方案,用于物联网中的 N 次计算分流[20]	轻量级的密钥协商场景	密钥分层方式	对称方式完成密钥协商速度较快,适用于低性能物联网设备.但没有解决不同密钥中心下的设备之间的密钥共享问题.
	边缘计算网络中用于多服务器体系结构的具有隐私保护属性的端到端认证密钥交换协议[21]	多服务器密钥协商	终端和边缘服务器通过共享方式协商密钥,服务器之间通过公钥方式协商密钥	密钥协商简单,适用于多服务器场景,未能给出形式化的安全性证明.
	雾计算环境下的安全密钥管理方案[22]	轻量级密钥协商	使用 Hash 及对称密钥完成协商	仅使用口令结合 Hash 方式完成密钥共享.但对称的方式中,口令很容易遭受离线字典攻击
	基于雾的抗量子轻量级认证和密钥协商协议[23]	抗量子密钥协商	利用利用经典的 Random-HB 协议完成	将密钥协商的安全性规约到基于带噪声校验学习(the learning parity with noise, LPN)问题,抗量子分析.

2) 对称密钥协商.对称的密钥协商本质上是以密钥分层方式来完成,即往往由主密钥衍生出多个子密钥给边缘节点或者终端,设备之间通过共享的子密钥完成密钥协商.Wang 等人[20]通过向用户设备以及边缘计算设备嵌入共享密钥的方式来完成认密钥协商.由一个种子密钥衍生出不同凭证分发给用户终端以及边缘节点.密钥协商过程使用抗泄露智能卡(攻击者攻陷智能卡后不能获得智能卡内的秘密信息),因此在拥有共享密钥的情况下可以使用对称加密以及消息认证码的方式完成密钥的协商.对称的方式速度快效率高,较适合低性能的物联网设备.但同一密钥中心下基于该中心的密钥可以完成密钥共享,如何完成不同密钥中心下的密钥共享是一个问题,因为不同中心下的设备往往不能共享密钥凭证.其他对称方式完成的密钥协商方案有 Hsu 等人[21]提出的多服务器场景的密钥协商,Wazid 等人[22]提出的仅使用 Hash 函数完成的密钥协商.基于 Hash 的方式往往结合口令一起形成密钥协商.具体方法是采用形如 $H(PW,\cdots)$ 的方式共享密钥凭证,其中 H 为 Hash 函数,PW 为用户口令.在进行密钥协商时可以采用密钥凭证结合随机数的方式,也可以采用密钥凭证结合 Diffie-Hellman 密钥协商的方式完成.2 种方法的区别是后面一种方法通过增加少量指数运算可以实现前向安全属性(攻击者获得当前用户的长期密钥后也不能计算出在该节点之前用户协商的会话密钥).除此之外也有一些特殊的边缘计算密钥协商协议,如抗量子密钥协商协议[23]以及使用物理不可克隆函数的密钥协商协议[24].在边缘计算环境下考虑这些特殊的密钥协商协议有助于进一步拓展边缘计算的应用场景.

3) 边缘计算密钥协商协议总结.边缘计算密钥协商协议目前仍大多数采用传统的密钥协商方式,无论是采用密钥分层方式还是基于凭证的方式都没有解决物联网设备需要进行频繁的数据交换从而导致密钥频繁协商的问题.当大规模边缘节点和终端进行密钥协商时,已有密钥协商协议则可能出现效率上或者安全上的问题.因此,需要结合新的密钥分发机制来解决,如边缘计算群组密钥协商或者基于可信计算的密钥协商等.对于不同场景的边缘计算密钥协商也需进一步完善,如需要频繁密钥交换时的密钥

协商或者只是需要偶然密钥交换的密钥协商等.

2.3 边缘计算环境下隐私保护协议

隐私保护是网络通信所需要考虑的重要安全问题之一.边缘计算环境下需要对用户以及终端隐私进行保护,保护身份、位置以及数据隐私[25].针对保护的信息不同,将边缘计算隐私保护协议分为身份及位置等隐私保护以及数据隐私保护两大类.表 5 及表 6 给出了不同隐私保护方案的分类、分析和总结.

Table 5 Privacy-Preserving Protocols for Identity and Location in Edge Computing Environments

表 5 边缘计算环境下身份及位置隐私保护协议

方案	解决问题	技术方法(模式)	优劣势
移动边缘云环境下具有隐私保护的身份验证方案[26]	身份信息保护	利用公钥产生对称密钥后加密身份信息	方法简单,性能高.但仅支持单一身份认证时隐私保护,无法提供批量认证时的隐私保护.
车联网中基于边缘计算的匿名认证方案[27]	身份及位置信息保护	使用匿名凭证,类似零知识证明对隐私进行保护	方法新颖,不同于以往密码算法.缺点是匿名凭证常使用双线性对,方案复杂,效率上有一定妥协.
轻量级的具有隐私保护的物联网的健康存储方案[28]	具有消息聚合的身份信息保护	基于假名机制实现匿名,使用依聚合性质的签名聚合消息	假名机制实现匿名方法简单,且考虑了消息聚合.但该方案没有考虑边缘计算环境下多个域时如何对假名进行处理.
雾计算环境下车联网的隐私保护假名方案[29]	假名动态更新及分发	根据上下文等信息动态更改假名	考虑了假名的动态更新问题,避免频繁使用假名泄露用户隐私.

Table 6 Privacy-Preserving Protocols for Data in Edge Computing Environments

表 6 边缘计算环境下数据隐私保护协议

方案	解决问题	技术方法(模式)	优劣势
基于计算智能的 3 层隐私保护云存储方案[30]	分层的数据存储隐私	基于 Hash-Solomon 编码将存储数据分成 3 部分分别存储在多个实体中	将数据进行分层保存到云—边—端,数据隐私得到保护.但仍需进一步考虑云—边—端的同步问题.
基于边缘计算的差分隐私方案[31]	分层的数据存储隐私	使用差分隐私保护数据隐私	数据分层存储,健壮性强.使用差分隐私避免复杂密码运算.
基于雾的智能电网的隐私保护数据聚合方案[32]	边缘环境下数据聚合	传统同态加密	数据可以加密后聚合,但使用同态加密效率较低.
轻量级且可验证的隐私保护数据聚合方[33]	轻量级数据聚合	Paillier 同态加密	数据可以加密后聚合,使用效率较高的同态加密算法.
雾计算中动态的隐私保护数据聚合方案[34]	终端动态变化时的数据聚合	非同态加密,产生伪随机比特流对数据加密后聚合	非同态加密的聚合加密算法,避免使用大规模运算,其安全性仍有待进一步验证.
移动边缘计算下车联网隐私保护方案[35]	数据既需要签名又需要具有加密	签密算法	签密方法既可加密又可签名,方法新颖,但复杂度较高.
边缘计算中基于差分隐私的数据隐私保护算法[36-37]	数据不加密情况下的隐私保护	差分隐私	使用差分隐私避免复杂密码运算.差分隐私在得到大规模训练数据后能否泄露隐私仍有待验证.
边缘计算环境下大数据训练模型的差分隐私保护[38]	机器学习时保证数据隐私	差分隐私	在机器学习背景下进行差分隐私,即考虑了差分隐私的强度.

1) 身份及位置等隐私保护.边缘计算提供了本地化的资源和服务,满足了用户和设备实时处理的需求.但边缘计算环境下存在多个不同的安全域,用户在不同安全域的边缘计算网络中访问资源或请求服务时需要保证其身份、位置等隐私不被泄露.Liu 等人[26]针对移动边缘云架构,提出了一种具有隐私保护的双向认证方案,并把该方案应用在医疗健康领域.文献[26]的方案在云—边—端环境下使用双重匿名将用户身份信息隐藏,隐私保护方法可以看成是通过临时公钥产生共享密钥后加密身份等隐私信息.Guo 等人[27]提出了在车联网和家庭网络之间基于边缘计算的匿名认证方案.不同于以往的隐私保护方案,文献[27]采用的是基于匿名凭证(anonymous credential)的方式实现身份及车辆位置隐私.匿名凭证的优点是不仅不会泄露用户隐私给攻击者,同时对于验证者来说在保证其验证通过的情况下也不泄露隐私给验证者.这样的方式相当于实现了零知识证明的效果.然而匿名凭证的使用往往需要大量的

双线性对运算,虽然其对于隐私保护起到重要作用,但仍需进一步寻找更有效的匿名凭证方案.

对于用户身份保护常用的方式即是通过一个假名来代替某个用户的真实身份,通过频繁更换假名来实现用户身份的隐私保护.Ding 等人[28]提出在医疗边缘网络环境中使用假名保护患者身份的方案.用户的医疗数据通过传感器发送给边缘节点,边缘节点对数据进行聚合后再发送给云中心,数据聚合后结合假名机制保护用户隐私.但边缘计算网络是无中心的结构,同时存在不同的假名管理域(一个边缘计算节点和其附近终端可以看成一个域).每个边缘节点为其附近终端分配假名,而非由云中心分配假名.这样不同域间的假名频繁更换以及分发,如何保证效率以及如何在隐私保护下进行认证也是一个问题.Kang 等人[29]提出了边缘车联网计算环境下具有更多功能的假名方案.其优点是可以通过上下文信息感知来更改假名,同时可以及时分发假名减少假名管理的开销.

2) 数据隐私保护.边缘计算环境下数据无论是传输到边缘节点还是通过便于节点传输到云中心都需要实现数据的隐私保护.Wang 等人[30]考虑云—边—端环境下数据存储隐私问题,即数据存储在云中即使加密后处理也可能会遭受内部攻击.在里所编码(Reed-Solomon)的基础上设计了 Hash-Solomon 编码,从而将用户数据分成 3 个部分,即由云、边以及终端各自存储一部分数据.即使有任意一部分数据被泄露攻击者也不能恢复完整的数据,从而保护数据隐私.Wang 等人[31]同样考虑数据存储隐私问题,利用差分隐私的方法对数据进行分离,将一部分数据存储在边缘节点、一部分存储在云中,从而保证数据一部分丢失攻击者也不会恢复全部数据.

数据隐私保护最直接的方法就是对数据进行加密后传输或存储.简单地对每个密文单独处理会导致边缘节点处理大量密文,因此需要在边缘节点处对密文数据进行聚合处理.同态加密(homomorphic encryption)具有密文同态性质可以对数据进行聚合处理从而实现数据隐私保护.Zhao 等人[32]基于同态加密提出了智能电网边缘计算环境下的用户数据隐私保护方案.通过在边缘计算处进行同态加密对数据进行聚合处理,在保证效率的同时也保护了用户用电隐私.Zhang 等人[33]提出基于 Paillier 同态加密的轻量级同态加密方案,更适用于边缘计算环境.同时,通过一种离线/在线签名方案使得大计算量的运算被卸载到边缘计算节点,从而减轻物联网设备负担.

同态加密运算量较大,学者探索不使用同态加密的数据隐私保护方案.为解决终端节点的频繁流动问题,Shen 等人[34]提出了动态的数据聚合方案.没有使用传统的同态加密方案,文献[34]提出了一种可以进行多种密文操作的加密方案.其基本思想是通过一个伪随机函数生成一个和时间相关的伪随机比特流,然后用该比特流加密数据再进行聚合.考虑到终端节点对消息既要加密又要签名,Rasheed 等人[35]使用签密方案对数据进行处理,签名后再进行数据的聚合处理.

隐私保护大都是通过密码算法对身份信息进行保护或者通过假名来实现隐私保护,这样的方式需要对数据进行加密,且复杂度较高,可以采用差分隐私的方法实现隐私保护.Qiao 等人[36]指出边缘计算的优势在于数据共享而非加密,应考虑在数据以明文存在的情况下保护用户隐私.其提出采用差分隐私的方法保护用户隐私数据.具体方法是采用基于贪心算法的分区算法来获得更好的分区结构,然后使用小波变换增加噪音,从而实现数据的带噪发布.Jing 等人[37]基于差分隐私方法给出了当边缘计算节点被攻陷时如何保证数据隐私.为了避免使用差分隐私后造成的部分数据丢失,其采用线性规划实现最优位置模糊矩阵的选择,并采用数据丢失和重构方法使数据不确定性最小化.边缘节点靠近用户终端,其会搜集大量用户信息,因此在边缘节点处利用机器学习等人工智能方法可以进一步挖掘出数据背后的价值.然而使用机器学习对数据分析时可能会泄露用户隐私.Du 等人[38]考虑在机器学习环境下的用户隐私方案,基于差分隐私方式保证了当数据被用来学习时也不会泄露用户隐私.

3) 边缘计算隐私保护协议总结.已有边缘计算隐私保护侧重采用密码学手段对数据进行加密处理,基本解决了性能良好设备条件下的隐私保护.但仍需考虑在终端及边缘节点的计算能力有限的情况下如何进行隐私保护.一种解决方法是可以使用其他非传统密码手段实现隐私保护,如差分隐私方法保护用户隐私.差分隐私不需要复杂的密码学运算,这尤其适用于性能受限的物联网设备.同时边缘计算的优势在于数据的频繁交互及共享,若每次都对数据进行加密处理来保护隐私将大大削弱边缘计算的优势.差分隐私虽然可以实现数据半公开情况下的

隐私保护,但随着机器学习等人工智能算法的出现,当大量样本出现时能否仍能依赖差分隐私来实现边缘计算网络中用户即终端设备隐私保护仍然是一个问题.

2.4 边缘计算环境下数据共享协议

边缘技术最大的优点是提高数据的使用和处理效率,因此如何在边缘计算中实现安全的数据共享是一个重要的研究内容.数据在什么情况下以什么形式共享是边缘计算所要解决的重要问题.根据数据共享时使用的技术方法不同,将数据共享协议分为3类并进行总结.

1) 基于属性加密数据共享.数据共享权限往往通过访问控制机制来实现.而传统的访问控制不能抵抗边缘服务器有意无意的泄露用户数据.在边缘计算环境中引入属性加密(attribute-based encryption)可以解决这个问题.根据不同用户属性,将密文同属性相结合,只有满足一定属性的用户才能共享数据.

基于此,Pan 等人[39]在边缘车联网环境下设计了基于属性加密的数据共享方法.由性能良好的车辆充当边缘节点的角色(可以看成不固定边缘计算节点),共享数据由边缘计算节点传送给满足密文属性的请求者.这样在保证数据快速共享的同时实现灵活的访问控制.由于边缘计算环境中设备往往存在不同域中,需要解决在不同域下的数据共享问题.Fan 等人[40]基于密文策略属性加密给出了跨域场景下的数据共享方案.基于传统的属性加密方案,利用云中心作为不同域的中间可信节点完成数据共享.但该方案仍没有脱离云中心,需要云中心协助处理数据共享.同时在基于属性加密方案中仍需考虑用户不具备每个属性后应该采取一种有效的方法取消其解密资格.Pu 等人[41]将区块链引入边缘计算数据共享中,利用属性撤销链将用户身份和属性的Hash值存储到链中,利用区块链的不可篡改性完成属性撤销鉴别.即当用户提出数据访问请求时,边缘计算节点首先验证其是否在属性撤销链中,当其信息在链中时拒绝数据请求.但其未考虑当其他有权限的用户请求数据时,撤销属性的用户是否可以通过某种方式获得密文从而利用之前的密钥顺利解密,即用户绕过属性撤销列表获得密文时的情况.Vohra 等人[42]考虑属性加密的前向安全性,即新加入的成员不能解密之前密文的加密,同时考虑后向安全性,即成员退出时也不能解密后面的密文.利用属性加密和代理重加密算法提出了边缘计算环境下的数据安全共享方案.在基于属性加密的数据共享时,一些属性往往跟时间有关,如在上班时间某些员工可以访问一些数据,但是其他时间不可以访问.因此,需要将时间属性引入属性加密中.基于此,Li 等人[43]考虑边缘计算环境下带有时间域的数据共享方案.密文在边缘计算节点中进行预解密处理,然后交给终端节点进行具体解密,在这个过程中加入时间属性条件并考虑了时间属性更新问题.

2) 基于代理重加密数据共享.代理重加密(proxy re-encryption)可以实现将密文由代理节点通过代理密钥转换为另外一份密文从而由他人解密.Wang 等人[44]提出通过基于身份的代理重加密方法实现安全的数据共享方案.边缘计算节点通过代理重加密密钥将密文重新加密后发送给终端,终端利用私钥顺利进行解密.考虑分布式边缘计算和环境中使用代理重加密需要验证多个终端公钥的真实性问题,Gao 等人[45]采用区块链技术提出了基于区块链的数据共享方案.将用户公钥证书放到区块链中,结合区块链不可篡改以及公开可验证的优点完成公钥真实性验证.为了解决数据共享时数据发布者的身份隐私问题,Cui 等人[46]结合群签名和代理重加密机制实现了边缘计算环境下匿名的数据共享方案.数据发布者以群成员的身份加入群中,对数据进行群签名,然后再进行加密后发给边缘节点.边缘节点利用代理重加密密钥对密文进行重加密后发给数据请求者,数据请求者利用自己的私钥顺利解密.为了使由不同物联网设备收集来的数据得以安全聚合,Huang 等人[47]基于同态代理重加密(homomorphic proxy re-encryption)机制提出了具有隐私保护的数据聚合方案.为了解决边缘计算节点因某些利益可能会仅聚合部分数据的问题,文献[47]利用随机线性同态签名算法使得边缘计算节点不能随意聚合数据.但随机线性同态签名计算量较大,该算法能否部署在实际的边缘计算节点仍有待进一步考证.

考虑边缘计算节点在进行代理重加密时使用公钥密码所导致的计算量大的问题,Khanshan[48]提出了对称密码和公钥密码相结合的混合代理重加密.终端利用对称密钥加密明文消息,然后利用代理加密机制加密对称密钥,边缘计算节点根据代理重加密密钥对加密后的对称密钥进行转换得到新的密文.数据请求者根据自己的私钥对对称密钥密文进行解密获取对称密钥,最后对消息进行解密.该过程类似数字信封过程.

3) 基于机器学习数据共享. 随着人工智能技术

的发展,使用机器学习等方法对数据进行处理分析从而得出更有效的信息是目前的主流方法之一.用户把自己的数据共享出来从而被多个机构去学习应用.然而数据往往需要隐私保护,如何保证用户数据在密文的形态下实现数据的训练是数据共享要解决的关键问题.联邦学习(federated learning)[49]的提出解决了上述问题.利用同态加密等方法可以实现对密文进行学习,其在保证用户数据隐私的情况下达到和对明文学习相同的效果.在边缘计算数据共享中更加需要联邦学习机制,因为边缘计算环境中边缘设备往往属于不同域,域与域之间是不可信的,不同域间共享数据更需要隐私保护.同时与传统机器学习方式不同,联邦学习不需要集中所有数据后进行学习,这更适合分布式的边缘计算环境.

Lim 等人[50]给出了移动边缘计算环境下联邦学习综述,介绍了边缘计算与联邦学习结合的优势、存在问题以及解决方法.Albaseer 等人[51]考虑在城市边缘计算环境下的数据共享学习问题.使用半监督模型解决城市边缘环境中有标记数据少而未标记数据多的问题.由于联邦学习使用同态加密,在边缘计算环境下进行密文学习提升其学习效率是一个重要问题.利用区块链技术,Cui 等人[52]将区块链与联邦学习结合提出基于区块链的联邦学习机制.利用区块链的不可篡改特性存储终端数据到区块链中,边缘计算节点利用联邦学习模型对数据进行学习后再上传到云中心,最后由云中心继续进行学习得出有效信息(如用户数据使用偏好等)后再分发到边缘节点,从而使得终端设备可以更加有效地共享数据.为了进一步提升联邦学习过程中的通信效率,芦效峰等人[53]通过调整参数对边缘节点和终端之间的冗余通信进行压缩以此提升通信效率.Wu 等人[54]和 Osia 等人[55]分别提出了分层的深度学习模型.即在云—边—端的网络架构中,边缘计算节点和云服务器分别对数据进行学习.由边缘计算节点完成神经网络的第 1 层处理,然后由云服务器完成剩余层的处理,这样的分布式处理进一步提升了学习效率.

4) 边缘计算数据共享协议总结.数据共享是边缘计算环境中最为重要的问题.利用复杂的密码学技术如属性加密以及代理重加密等方法,已有数据共享协议基本实现了数据共享的功能.但其使用的密码算法过于复杂,其适用于性能较好的边缘节点,但不适用于性能相对较低的终端节点.一方面,需要进一步提升使用的底层密码算法的效率,或者在其基础上进行改进使其更适用于边缘环境性能相对低的终端节点.具体来讲可以探索采用更多对称的方式完成数据共享,如代理重加密过程使用对称的方式完成等.另一方面,需要探索更多在明文状态下的数据共享方法.在什么情况下数据可以以明文状态下进行共享同时共享过程及共享结果仍是安全的,如何实现隐私保护等属性,这些问题仍需要在边缘计算环境中进行进一步的研究.

以上按照属性加密、代理重加密以及联邦学习方法将边缘计算数据共享协议进行了分类及总结,具体如表 7~9 所示.数据共享协议可以说是 4 类安全协议中最重要的协议,因为无论身份认证及密钥协商最终目标都是为了进行数据安全的传输及共享.而隐私保护则是数据共享时需要提供的一种安全属性.边缘计算环境下数据共享协议是边缘计算环境下安全协议研究的出发点及落脚点,需要进一步深入研究.

Table 7 Data Sharing Protocols Based on Attribute-based Encryption in Edge Computing Environments

表 7 边缘计算环境下基于属性加密的数据共享协议

方案	解决问题	技术方法(模式)	优劣势
边缘计算环境车联网数据共享方案[39]	边缘计算环境基于属性数据共享	不固定边缘计算节点结合属性加密	解决了单一域内数据安全共享,未解决边缘计算中不同域间数据共享.
边缘计算环境下跨域的数据共享方案[40]	跨域数据共享	传统属性加密+云中心作为不同域的可信中间节点	解决跨域数据共享,但仍然以需要云中心实时参与,未真正起到边缘计算作用.仍需进一步实现分布式跨域数据共享.
可恢复及可撤消的隐私保护边缘数据共享方案[41]	属性撤销安全	将用户身份和属性加入到区块链中,通过查看区块链验证属性	用户属性信息保留到区块链中,解决了对属性的安全验证问题.但仍考虑属性撤销用户绕过属性撤销列表获得密文而解密.
带有时间域的属性加密数据外包方案[42-43]	属性加密中时间域问题	属性加密中引入时间属性	将时间因素引入数据共享中,同时利用多授权的属性加密方案将计算任务卸载到边缘节点.其问题在于大量使用双线性对运算导致效率不高.

Table 8 Data Sharing Protocols Based on Proxy Re-encryption in Edge Computing Environments

表 8 边缘计算环境下基于代理重加密的数据共享协议

方案	解决问题	技术方法(模式)	优劣势
雾计算环境下基于抗泄露代理重加密的访问控制方案[44]	雾计算环境下的数据隐私保护	基于身份的代理重加密	边缘计算节点利用代理密钥将密文转换,效率较高.
支持软件定义网络的基于区块链的数据共享框架[45]	代理重加密中公钥真实性验证问题	代理重加密+区块链	在边缘节点采用代理重加密的方式完成密文转换,进一步完成数据共享.这样的方式很好地利用了边缘计算的特点.将公钥证书上链实现了分布式证书鉴别.
半信任边缘节点环境下匿名消息共享方案[46]	匿名数据共享	群签名+代理重加密	通过群签名的方式解决了数据共享时共享人的身份隐私保护.但群签名能否在物联网终端普通适用仍有待验证.需要轻量级的隐私保护协议.
具有保护隐私的可选择性数据聚合方案[47]	数据聚合隐私保护	同态代理重加密	使用同态代理重加密解决了不同终端机密数据的聚合问题,同时解决了有选择的数据聚合问题.理论上该方式是可行的,但如此高计算量部署在边缘节点对边缘节点的性能提出了一定挑战.
物联网环境下混合轻量级代理重加密方案[48]	代理重加密过程中高复杂度问题	代理重加密+数字信封	解决了采用代理重加密实现数据共享过程中高计算量问题.采用数字信封的方式完成对称密钥的共享.

Table 9 Data Sharing Protocols Based on Federated Learning in Edge Computing Environments

表 9 边缘计算环境下基于联邦学习的数据共享协议

方案	解决问题	技术方法(模式)	优劣势
移动边缘网络中的联邦学习综述[50]	联邦学习与边缘计算结合的优势、存在的问题	综述	给出了移动边缘计算综述.
智慧城市下未标记数据的联邦学习方案[51]	有标记数据少而未标记数据多的问题	半监督联邦学习模型	给出了特殊场景下联邦学习方法,采用半监督模型进行密文数据的学习.
边缘计算下用于内容缓存的基于区块链的联邦学习方案[52]	数据共享偏好快速识别问题	区块链+联邦学习	通过先检测用户偏好的方式更有效地实现数据共享.利用区块链不可篡改特性防止训练数据被篡改而得到错误结论.
面向边缘计算的高效异步联邦学习机制[53]	联邦学习通信效率	压缩冗余通信	解决联邦学习过程中大通信量问题.
移动边缘计算中终端联邦学习的加速方案[54-55]	联邦学习效率问题	分层联邦学习模型	边缘计算节点和云服务器分别对数据进行学习.由边缘计算节点完成神经网络的第1层处理,然后由云服务器完成剩余层的处理.分布式处理进一步提升了学习效率.

3 安全协议存在的问题及研究方向

3.1 存在的问题

针对边缘计算的安全需求,已有的安全协议解决了边缘计算环境下认证、密钥协商、隐私保护以及数据共享的基本问题,但仍存在4个共性问题需要进一步解决.

1) 安全协议凭证存储位置问题.边缘计算不是否定云计算,而是作为云计算的辅助网络结构以及计算结构.在考虑边缘计算场景下的安全协议时,对于实现不同安全需求,什么样的凭证保存在云端、什么样的凭证保存在边缘计算设备中目前没有一个公认的衡量标准.

2) 安全协议效率问题.已有的安全协议中数据及安全凭证以密文为主,通过复杂的密码工具如同态加密以及代理重加密等方式共享数据.但在边缘计算环境中如此大的计算量对于实际运行的终端及边缘节点是否可行、是否具有普遍的通用性,仍需进一步结合实际进行分析.

3) 安全协议计算任务卸载问题.边缘计算突出的优点是快速完成用户对物联网设备的应用需求.已有安全协议大都是将计算及通信任务放到边缘节点中完成.虽然边缘节点在一定程度上性能优于普通物联网终端节点,但其进行大量计算时性能也将受限.需要进一步探索如何安全高效地将计算任务卸载到其他边缘节点或者终端[56].何种场景以何种方式将计算任务卸载给其他边缘节点或者性能良好的终端也有待进一步研究.

4) 安全协议应用场景问题.由于车联网中设备相对具有较高的运算及存储效率,其上可以应用很多密码工具,因此已有的安全协议大部分集中在边

缘车联网中.但边缘计算应用场景广泛,车联网只是边缘计算的一个应用场景,仍需进一步研究在其他边缘计算应用场景中的安全协议.

3.2 研究方向

结合边缘计算环境下安全协议存在的问题及已有的安全协议成果,给出4个研究方向建议:

1) 探索采用分布式的安全凭证解决安全凭证的存储问题.将核心凭证或者长期保存的凭证仍存储在云中心,将临时凭证存储在边缘节点中,以此解决分布式认证需求.针对不同的安全需求,研究以形式化的方法去定义安全目标,进一步从理论上论证安全凭证的存储及使用过程安全,从而推动安全协议相关安全标准的制定.

2) 探索采用轻量级密码技术或者更多非密码技术来解决边缘计算安全协议效率问题.可以进一步挖掘区块链优势,引入区块链到安全协议中.将公钥证书写入区块链减轻公钥的验证仅仅是一个方向,仍可探索将更多的数据写入区块链从而解决安全协议运行时各方的效率和信任问题.边缘计算核心是数据的频繁应用,需要探索绕开复杂的密码技术实现数据安全应用,如采用可信模块、抗机器学习差分隐私、信任管理等技术实现安全协议的需求.

3) 探索采用多种途径多种技术解决边缘计算数据卸载问题.安全协议执行过程中有些任务可以卸载到边缘服务器节点,有些任务也可以卸载到物联网终端节点.可以探索更多任务卸载到终端设备,如认证过程的计算卸载以及数据共享过程的计算卸载,从而实现更灵活的计算.此外,为解决数据卸载时的公平性以及收益分配问题,可以进一步结合智能合约技术使得数据卸载过程不可篡改并可溯源,避免卸载后矛盾的产生.

4) 探索结合5G、人工智能等技术解决边缘计算安全协议应用场景扩展问题.可进一步探索结合5G的移动边缘计算场景下的安全协议,如智慧城市边缘计算网络安全协议、智慧医疗边缘计算网络安全协议以及智慧家庭及社区边缘计算网络安全协议.此外随着人工智能深入到各个领域,将边缘计算安全协议和人工智能结合可拓展边缘计算的应用范围,推动边缘计算的进一步发展.

4 总 结

综述了边缘计算环境下认证协议、密钥协商协议、隐私保护协议以及数据共享协议的最新进展.对具有代表性的成果进行了分类及分析.总结了已有边缘计算环境下安全协议仍没有解决的问题.针对存在的问题,给出了具体的研究方向及建议,为从整体上把握边缘计算环境下安全协议给出了参考.

作者贡献声明:李晓伟对论文进行了总体的撰写;陈本辉和杨邓奇给出了边缘计算隐私保护协议和数据共享协议撰写方面的建议,并对论文进行了修改;伍高飞对联邦学习相关内容给出撰写建议并对论文的总体架构给出了意见.

参 考 文 献

[1] Shi Weisong, Cao Jie, Zhang Quan, et al. Edge computing: Vision and challenges [J]. IEEE Internet of Things Journal, 2016, 3(5): 637-646

[2] Zhang Jiale, Zhao Yanchao, Chen Bing, et al. Survey on data security and privacy-preserving for the research of edge computing [J]. Journal on Communications, 2018, 39(3): 1-21 (in Chinese)
(张佳乐, 赵彦超, 陈兵, 等. 边缘计算数据安全与隐私保护研究综述[J]. 通信学报, 2018, 39(3): 1-21)

[3] Grand View Research Inc. Edge computing market size, share & trends analysis report [OL]. [2021-05-01]. https://www.grandviewresearch.com/industry-analysis/edge-computing-market

[4] Dewanta F, Mambo M. A mutual authentication scheme for secure fog computing service handover in vehicular network environment [J]. IEEE Access, 2019, 7: 103095-103114

[5] Mishra D, Dharminder D, Yadav P, et al. A provably secure dynamic ID-based authenticated key agreement framework for mobile edge computing without a trusted party [J]. Journal of Information Security and Applications, 2020, 55(12): 1-9

[6] Jia Xiaoying, He Debiao, Kumar N, et al. A provably secure and efficient identity-based anonymous authentication scheme for mobile edge computing [J]. IEEE Systems Journal, 2020, 14(1): 560-571

[7] Li Yuting, Cheng Qingfeng, Liu Ximeng, et al. A secure anonymous identity-based scheme in new authentication architecture for mobile edge computing [J]. IEEE Systems Journal, 2021, 15(1): 935-946

[8] Zhang Jing, Zhong Hong, Cui Jie, et al. An extensible and effective anonymous batch authentication scheme for smart vehicular networks [J]. IEEE Internet of Things Journal, 2020, 7(4): 3462-3473

[9] Lin Y D, Truong D T, Ali A, et al. Proxy-based federated authentication: A transparent third-party solution for cloud-edge federation [J]. IEEE Network, 2020, 34(6): 220-227

[10] Cui Jie, Wei Lu, Zhang Jing, et al. An efficient message-authentication scheme based on edge computing for vehicular ad hoc networks [J]. IEEE Transactions on Intelligent Transportation Systems, 2019, 20(5): 1621-1632

[11] Zhang Jing, Zhong Hong, Cui Jie, et al. Edge computing-based privacy-preserving authentication framework and protocol for 5G-enabled vehicular networks [J]. IEEE Transactions on Vehicular Technology, 2020, 69(7): 7940-7954

[12] Liu Hong, Zhang Pengfei, Pu Geguang, et al. Blockchain empowered cooperative authentication with data traceability in vehicular edge computing [J]. IEEE Transactions on Vehicular Technology, 2020, 69(4): 4221-4232

[13] Zhong Hong, Pan Lei, Zhang Qingyang, et al. A new message authentication scheme for multiple devices in intelligent connected vehicles based on edge computing [J]. IEEE Access, 2019, 7: 108211-108222

[14] Wang Cong, Zhang Yiying, Chen Xi, et al. SDN-based handover authentication scheme for mobile edge computing in cyber-physical systems [J]. IEEE Internet of Things Journal, 2019, 6(5): 8692-8701

[15] Wang Qianpeng, Gao Deyun, Foh C H, et al. An edge computing-enabled decentralized authentication scheme for vehicular networks [C/OL] //Proc of the 13th IEEE Int Conf on Communications. Piscataway, NJ: IEEE, 2020 [2021-04-29]. https://ieeexplore.ieee.org/document/9149021

[16] He Debiao, Kumar N, Wang Huaqun, et al. A provably-secure cross-domain handshake scheme with symptoms-matching for mobile healthcare social networks [J]. IEEE Transactions on Dependable and Secure Computing, 2018, 15(4): 633-645

[17] Zhang Shijie, Lee J H. A group signature and authentication scheme for blockchain-based mobile-edge computing [J]. IEEE Internet of Things Journal, 2019, 6(5): 4557-4565

[18] Guo Shaoyong, Hu Xing, Guo Song, et al. Blockchain meets edge computing: A distributed and trusted authentication system [J]. IEEE Transactions on Industrial Informatics, 2019, 16(3): 1972-1983

[19] Wang Jing, Wu Libing, Choo K K R, et al. Blockchain-based anonymous authentication with key management for smart grid edge computing infrastructure [J]. IEEE Transactions on Industrial Informatics, 2020, 16(3): 1984-1992

[20] Wang Fei, Xu Yonjun, Zhu Liehuang, et al. LAMANCO: A lightweight anonymous mutual authentication scheme for N-times computing offloading in IoT [J]. IEEE Internet of Things Journal, 2019, 6(3): 4462-4471

[21] Hsu C, Le T, Lu C, et al. A privacy-preserved E2E authenticated key exchange protocol for multi-server architecture in edge computing networks [J]. IEEE Access, 2020, 8: 40791-40808

[22] Wazid M, Das A K, Kumar N, et al. Design of secure key management and user authentication scheme for fog computing services [J]. Future Generation Computer Systems, 2019, 91(2): 475-492

[23] Lu Shouqin, Li Xiangxue. Quantum-resistant lightweight authentication and key agreement protocol for fog-based microgrids [J]. IEEE Access, 2021, 9: 27588-27600

[24] Gope P, Sikdar B. An efficient privacy-preserving authenticated key agreement scheme for edge-assisted internet of drones [J]. IEEE Transactions on Vehicular Technology, 2020, 69(11): 13621-13630

[25] Zhou Jun, Shen Huajie, Lin Zhongyun, et al. Research advances on privacy preserving in edge computing [J]. Journal of Computer Research and Development, 2020, 57(10): 2027-2051 (in Chinese)
(周俊, 沈华杰, 林中允, 等. 边缘计算隐私保护研究进展 [J]. 计算机研究与发展, 2020, 57(10): 2027-2051)

[26] Liu Xiaoxue, Ma Wenping, Cao Hao. NPMA: A novel privacy-preserving mutual authentication in TMIS for mobile edge-cloud architecture [J/OL]. Journal of Medical Systems, 2019 [2021-04-29]. https://link. springer. com/article/10. 1007%2Fs10916-019- 1444-9

[27] Guo Nan, Zhao Cong, Gao Tianhan. An anonymous authentication scheme for edge computing-based car-home connectivity services in vehicular networks [J]. Future Generation Computer Systems, 2020, 106(5): 659-671

[28] Ding Ran, Zhong Hong, Ma Jianfeng, et al. Lightweight privacy-preserving identity-based verifiable IoT-based health storage system [J]. IEEE Internet of Things Journal, 2019, 6(5): 8393-8405

[29] Kang Jiawen, Yu Rong, Huang Xumin, et al. Privacy-preserved pseudonym scheme for fog computing supported internet of vehicles [J]. IEEE Transactions on Intelligent Transportation Systems, 2018, 16(3): 1972-1983

[30] Wang Tian, Zhou Jiyuan, Chen Xinlei, et al. A three-layer privacy preserving cloud storage scheme based on computational intelligence in fog computing [J]. IEEE Transactions on Emerging Topics in Computational Intelligence, 2018, 2(1): 3-12

[31] Wang Tian, Mei Yaxin, Jia Weijia, et al. Edge-based differenital privacy computing for sensor-cloud systems [J]. Journal of Parallel and Distributed Computing, 2019, 136(2): 75-85

[32] Zhao Shuai, Li Fenghua, Li Hongwei, et al. Smart and practical privacy-preserving data aggregation for fog-based smart grids [J]. IEEE Transactions on Information Forensics and Security, 2021, 16: 521-536

[33] Zhang Jiale, Zhao Yanchao, Wu Jie, et al. LVPDA: A lightweight and verifiable privacy-preserving data aggregation scheme for edge-enabled IoT [J]. IEEE Internet of Things Journal, 2020, 7(5): 4016-4027

[34] Shen Xiaodong, Zhu Liehuang, Xu Chang, et al. A privacy-preserving data aggregation scheme for dynamic groups in fog computing [J]. Information Sciences, 2019, 514(4): 118-130

[35] Rasheed I, Zhang Lin, Hu Fei. A privacy preserving scheme for vehicle-to-everything communications using 5G mobile edge computing [J]. Computer Networks, 2020 [2021-04-29]. https://www.sciencedirect.com/science/article/abs/pii/S1389128619315658

[36] Qiao Yi, Liu Zhaobin, Lv Haoze, et al. An effective data privacy protection algorithm based on differential privacy in edge computing [J]. IEEE Access, 2019, 7: 136203-136213

[37] Jing Weipeng, Miao Qiucheng, Song Houbing, et al. Data loss and reconstruction of location differential privacy protection based on edge computing [J]. IEEE Access, 2019, 7: 75890-75900

[38] Du Miao, Wang Kun, Xia Zhuoqun, et al. Differential privacy preserving of training model in wireless big data with edge computing [J]. IEEE Transactions on Big Data, 2020, 6(2): 283-295

[39] Pan Jingwen, Cui Jie, Wei Lu, et al. Secure data sharing scheme for VANETs based on edge computing [J]. EURASIP Journal on Wireless Communications and Networking, 2019 [2021-04-29]. https://link.springer.com/article/10.1186/s13638-019-1494-1

[40] Fan Kai, Pan Qiang, Wang Junxiong, et al. Cross-domain based data sharing scheme in cooperative edge computing [C]//Proc of the 4th IEEE Int Conf on Edge Computing. Piscataway, NJ: IEEE, 2018: 87-92

[41] Pu Yuwen, Hu Chunqiang, Deng Shaojiang, et al. R2PEDS: A recoverable and revocable privacy-preserving edge data sharing scheme [J]. IEEE Internet of Things Journal, 2020, 7(9): 8077-8089

[42] Vohra K, Dave M. Securing fog and cloud communication using attribute based access control and re-encryption [C]//Proc of the 2nd Int Conf on Inventive Communication and Computational Technologies. Piscataway, NJ: IEEE, 2018: 307-312

[43] Li Youhuizi, Dong Zeyong, Sha Kewei, et al. TMO: Time domain outsourcing attribute-based encryption scheme for data acquisition in edge computing [J]. IEEE Access, 2019, 7: 40240-40257

[44] Wang Zhiwei. Leakage resilient ID-based proxy re-encryption scheme for access control in fog computing [J]. Future Generation Computer Systems, 2018, 87(10): 679-685

[45] Gao Ying, Chen Yijian, Hu Xiping, et al. Blockchain based IIoT data sharing framework for SDN-enabled pervasive edge computing [J]. IEEE Transactions on Industrial Informatics, 2021, 17(7): 5041-5049

[46] Cui Jie, Wang Fengqun, Zhang Qingyang, et al. An anonymous message authentication scheme for semi-trusted edge-enabled IIoT [J]. IEEE Transactions on Industrial Electronics, 2020 [2021-04-30]. https://ieeexplore.ieee.org/document/9269472

[47] Huang Cheng, Liu Dongxiao, Ni Jianbing, et al. Reliable and privacy-preserving selective data aggregation for fog-based IoT [C/OL] //Proc of the 11th IEEE Int Conf on Communications. Piscataway, NJ: IEEE, 2018 [2021-04-30]. https://ieeexplore.ieee.org/document/ 8422445

[48] Khanshan O A. Hybrid lightweight proxy re-encryption scheme for secure fog-to-things environment [J]. IEEE Access, 2020, 8: 66878-66887

[49] Wang Shiqiang, Tuor T, Salonidis T, et al. Adaptive federated learning in resource constrained edge computing systems [J]. IEEE Journal on Selected Areas in Communications, 2019, 37(6): 1205-1221

[50] Lim W Y B, Luong N C, Hoan G, et al. Federated learning in mobile edge networks: A comprehensive survey [J]. IEEE Communications Surveys & Tutorials, 2020, 22(3): 2031-2063

[51] Albaseer A, Ciftler B S, Abdallah M, et al. Exploiting unlabeled data in smart cities using federated edge learning [C]//Proc of the 16th Wireless Communications and Mobile Computing. Piscataway, NJ: IEEE, 2020: 1666-1671

[52] Cui Laizhong, Su Xiaoxin, Ming Zhongxing, et al. CREAT: Blockchain-assisted compression algorithm of federated learning for content caching in edge computing [J]. IEEE Internet of Things Journal, 2020 [2021-05-01]. https://ieeexplore.ieee.org/document/9159643

[53] Lu Xiaofeng, Liao Yuying, Pietro L, et al. An asynchronous federated learning mechanism for edge network computing [J]. Journal of Computer Research and Development, 2020, 57(12): 2571-2582 (in Chinese)
(芦效峰, 廖钰盈, Pietro Lio, 等.一种面向边缘计算的高效异步联邦学习机制[J]. 计算机研究与发展, 2020, 57(12): 2571-2582)

[54] Wu Wentai, He Ligang, Lin Weiwei et al. Accelerating federated learning over reliability-agnostic clients in mobile edge computing systems [J]. IEEE Transactions on Parallel and Distributed Systems, 2021, 32(7): 1539-1551

[55] Osia S A, Shamsabadi S, Sajadmanesh S, et al. A hybrid deep learning architecture for privacy-preserving mobile analytics [J]. IEEE Internet of Things Journal, 2020, 7(5): 4505-4518

[56] Zhang Qiuping, Sun Sheng, Liu Min, et al. Online joint optimization mechanism of task offloading and service caching for multi-edge device collaboration [J]. Journal of Computer Research and Development, 2021, 58(6): 1318-1339 (in Chinese)
(张秋平, 孙胜, 刘敏, 等. 面向多边缘设备协作的任务卸载和服务缓存在线联合优化机制[J]. 计算机研究与发展, 2021, 58(6): 1318-1339)

Li Xiaowei, born in 1985. PhD, associate professor. His main research interests include security protocol, blockchain and cryptography.

李晓伟,1985 年生.博士,副教授.主要研究方向为安全协议、区块链以及密码学.

Chen Benhui, born in 1978. PhD, professor, PhD supervisor. His main research interests include machine learning, data mining, and information security.

陈本辉,1978 年生.博士,教授,博士生导师.主要研究方向为机器学习、数据挖掘、信息安全.

Yang Dengqi, born in 1979. PhD, professor. His main research interests include machine learning and information security.

杨邓奇,1979 年生.博士,教授.主要研究方向为机器学习和信息安全.

Wu Gaofei, born in 1987. PhD, lecturer. His main research interests include sequences design and cryptography.

伍高飞,1987 年生.博士,讲师.主要研究方向为序列设计和密码学.