智能电网中数据聚合与用户查询隐私保护研究

王冰尧

广州华立学院 广州

【摘要】近年来，随着电力行业的飞速发展，智能电网企业的核心业务和支柱技术得到了越来越多的关注。由于各种原因，电力行业与互联网融合后产生了大量数据。在大数据时代，如何对海量数据进行有效挖掘、高效处理与管理成为各国关注的重点。随着信息技术与能源互联网的发展应用使大量信息集中在一起形成海量数据，这些数据需要经过挖掘、清洗、分析得到有效应用。然而，由于传统数据管理方式对隐私保护不够重视和专业知识不足等问题导致在互联网时代中，隐私问题突出，其危害十分严重。由于用户或系统对自身信息的依赖程度非常高，即使在互联网时代人们也不愿意让自己的隐私遭受到损害。本文以配电自动化系统为例研究了智能电网中用户查询隐私保护问题研究及其实施方案。

【关键词】智能电网；数据聚合；用户查询

【收稿日期】2022 年 11 月 12 日 【出刊日期】2022 年 12 月 21 日 【DOI】10.12208/j.aics.20220077

Research on data aggregation and user query privacy protection in smart grid

Bingyao Wang

Guangzhou Huali College, Guangzhou, Guangdong

【**Abstract**】In recent years, with the rapid development of the power industry, the core business and Pillar Technology of Smart Grid Enterprises has received more and more attention. For a variety of reasons, the power industry and the Internet after the integration of a large number of data. In the era of big data, how to effectively mine, efficiently process and manage the massive data has become the focus of attention. With the development and application of information technology and Energy Internet, a large amount of information is gathered together to form a mass of data, which needs to be mined, cleaned and analyzed to be effectively applied. However, due to the lack of attention to privacy protection and the lack of professional knowledge in traditional data management, the problem of privacy becomes more and more serious in the internet age. Because users or systems rely so heavily on their own information, even in the internet age people are reluctant to compromise their privacy. This paper takes distribution automation system as an example to study the research and implementation of user query privacy protection in smart grid.

【**Keywords**】smart grid; data aggregation; user query

引言

伴随着科技的发展和社会的不断进步，传统电力系统已经无法满足能源利用效率，安全稳定等要求。伴随着技术的进步，各种新技术将不断涌现，这些新技术将伴随着技术进步应运而生，比如人工智能，密码学，区块链和大数据。智能电网是集信息技术，基础结构和控制技术于一体的电网运行新机制。现阶段，智能电网已经广泛应用到通信技术，现代控制理论和计算机技术，并且在某种程度上满足了现阶段能源发展对电网的要求。然而，在智能电网蓬勃发展的同时，伴随而来的是数据隐私泄漏问题。所以如何设计出高效，高效的保护网络信息系统是当前智能电网运行中的关键问题。通常情况下，智能电网可以从能量流，信智能电网组成主体来看，主要有分布式能源发电厂，集中式能源发电厂，电动汽车和大众消费群体等；从信息流角度来看，智能电网主要由智能采集终端，存储中心，控制中心和通讯网络组成；从业务流程角度分析，智

能电网结构实体由聚合器，密钥分配中心和轻型终端装置组成。由上述分析可知，智能电网中有海量数据，一旦泄露，将会产生巨大的影响。智能电网运行机制下，有海量电力数据，电力通信过程数据和用户身份信息。由于电网本身具有易碎性、易受攻击性等特点，使得其在传输、存储等环节都会出现大量数据泄漏现象，进而对电网造成了极大安全隐患。从业务流程，业务流程三个方面展开分析。

1 智能电网隐私保护研究现状

1.1 智能电表身份隐私保护技术

当前智能电网下个人隐私保护主要有以下几个方面：智能电表使用者隐私保护，电动汽车位置和存储，电力通信数据个人隐私保护，电力数据个人隐私保护以及能源交易个人隐私保护。智能电表用户隐私保护重点关注其生成电力实时数据的安全保护。智能电表能够实时采集用户用电量并反馈至数据中心。通过对数据中心数据进行分析，能够实时了解电网负载情况，以便制定出相关调度策略。然而通过智能电表收集到的近实时电力消耗信息也会造成数据隐私性泄露。一旦遭到攻击者窃取，不仅影响了个人隐私权，也给电力系统带来了不可逆的破坏，严重影响了人们日常生活。如果不能够有效应对上述问题，就会在很大程度上对智能电网产生影响，甚至使智能电网发展停滞不前。智能仪表身份保护技术，就是研究其身份与隐私权保护问题。尽管攻击者能够通过用户智能仪表获得与用户有关的信息，但是并不能准确查找到用户，更加不能得到他们的真实身份来保护他们的个人隐私。目前身份保密技术种类繁多，包括电子签名，数字证书和零知识证明。2011 年 JAWUREK 等为智能电网增加部分隐私元件来保证数据隐私权不外泄。该方案的秘密元件只向能源厂商提供账单资料，无其他有效信息。2018 年，赵乙桥提出了一种新的方案，该方案采用了一种基于聚合签名技术的无证环签名方案，该方案不仅具有较小的计算量，而且具有非常好的隐私性。近年来，个人信息保密技术研究有不少突出成果。2019 年 ZHANG 等提出了一种轻量级的，匿名的，可用于智能电力网的密钥协商方案，使得智能电表和业务提供商能够相互验证，并在彼此之间建立共享的会话密钥。2020 年 KONG 等为智能电网保密群盲签名方案。

1.2 智能电表数据隐私保护技术

（1）密码学技术在智能电表数据隐私保护上的应用

密码技术就是通过计算机运算复杂性对明文进行加密。当前应用最为广泛的 3 种技术分别为基于性质加密，同态加密和双线性对映技术。基于属性加密技术（ABE）被广泛应用于智能电网中，主要应用于相关存取控制机制中，属性密码技术特征基加密技术可分为 KP-ABE 与密文策略属性基密码（CP-ABE）。CP-ABE 问题是当前国内外学者关注的焦点问题之一。该技术，若在密钥内嵌入一些属性，则破译密码时，需要满足具体属性才能被破译。2010 年，LEWKO 等提出了 CP-ABE 机制，该机制采用双线性群，从理论上证明了 CP-ABE 的安全性。2013 年，RUJ 等建立了一个分散的安全数据聚集和访问控制系统，该系统将同态加密和属性加密结合起来，从而使不同属性的用户能够在智能电网中存取不同属性的数据。2013 年 HUR 推出了基于策略的 CP-ABE 算法不仅可以保护用户敏感信息，并在保证访问控制策略安全性的同时，也可以把大部分加密操作传递给数据存储中心以降低接收方的计算负担。这些方法虽经精心设计，但是均是以控制中心的可靠性假设为前提，而现实中很难达到这类理想假设。同时上述方法运算复杂性高、通信负载大，所以针对有此不足的电力仪表终端目前尚无能够高效实现数据保密。因此，如何为无信任第三方设计出高效的隐私保护方案仍然是个巨大的难题。

（2）非密码学技术在智能电网数据隐私保护上的应用

从数据全生命周期来看，各种不同类型和不同级别的威胁使得用户共享数据越来越少。就数据保密而言，除了加密技术以外，非加密技术已经被广泛应用。目前策略安全技术包括区块链、干扰、压缩、边缘计算、隐私增强技术、布隆过滤、联邦学习。区块链技术、隐私增强技术和联合学习技术是目前最为高效的安全技术之一。当前，区块链技术在数据安全领域得到了广泛应用，主要表现在以下几个方面：去中心化，去信任化和防篡改。当前区块链技术应用于数据保密领域已取得很大成效。①区块链增强了信息的保密性。当前区块链在数据加密，身份认证，访问控制和可信执行方面均以数据加密为基础，这些加密包括可搜索加密，代理重加密，安全多方计算和属性加密。②数据完整性增强。并且针对数据完整性进行研究，

就是要保证数据的安全性，同时针对区块链等不可篡改帐簿的本质属性进行应用，对保持数据的完整性来说，就是一个十分有效且具有实际意义的研究工作。当前，提升区块链数据完整性主要采用云数据审计和可删除区块链两种方法。③区块链增加了数据的可用性。区块链能够有效地抵御单一节点失效的原因在于其能够采用分布式方法解决问题以提高信息系统鲁棒性。另外，基于区块链技术的分布式存储系统能有效提高数据可用性。就信息安全而言，加密技术的运用是其基本途径。目前多种技术联合应用已经成为目前学术界研究的一个热点问题。同时，伴随着科学技术的发展，各种各样的安全问题接踵而至。因此如何在现有条件下设计一套更安全高效的智能电网数据保密机制仍需深入研究。基于此，本文将重点关注智能电网隐私保护与用户隐私查询的研发。

2 智能电网中数据聚合隐私保护

2.1 智能电网中数据聚合隐私保护研究

公钥加密是目前智能电网使用最多的技术之一，所以公钥加密在数据融合过程中具有十分重要的地位。文章以某论文[1]为实例，提出了基于智能电网数据聚集式隐私保护系统，该系统包括设备层，雾层，云层以及电力服务系统四层，包括 KGC（KGC），智能电表（SM），雾结点（Fog），云节点（Cloud）以及电力业务部门（EPSI）。1）KGC 的作用在于密钥的生成与分发，KGC 运算能力较强，但是可靠性不是很高。2）智能电表收集用户电力实时信息并通过加密或者签名等方式传送给对应雾节点并被雾结点收集数据再等待汇聚。3）所述雾节点设置于智能仪表与云端节点间。雾结点利用身份认证技术认证智能电表，再通过细粒度聚合后基于该数据发送给云端节点。4）收到聚集密文后，云节点先利用认证技术认证雾状节点的身份，然后利用 Horner 法则进行二次聚合并最后把结果传输给电力部门。5）电力部门分析得到聚合密文后解密得到各子区总用电量。此外，供电部门还将数据通过云层通道传输到各个雾区节点，让用户可以随时掌握自身用电量情况，保证了用电透明性。该系统不仅能有效利用运算能力而且能节约储存资源，给用户带来了很好的用户体验。

2.2 智能电网中数据聚合隐私保护相关工作

基于此，VANDIJK 等人于 2010 年用一初等模式算法构造一简单全同态密码体制并将它的安全性降至寻找一逼近整数即隐藏整数近乘数。2011 年 LI 等以网状网路连接智能仪表组成树并用 Paillier 密码体制进行集成。2017 年 GAI 等提出基于张量法则的实数全同态加密混合运算。同态加密依据一个数学难题来加密数据，是建立在计算上无法区分的经典密码算法之一。同态密码最早于 1978 年被 RIVEST 等于。区别于传统加密算法，同态密码拥有计算、分析等功能，能极大地减少解密过程中需要的运算量并且还能保证授权对象只能得到数据计算结果而无法得到数。

2.3 智能电网数据聚合隐私保护未来发展趋势

所以近年来很多学者对智能电网中数据集聚隐私问题提出很多解决办法。如何在并行分布式架构，动态响应，有限终端资源，边缘大数据处理，人工智能协作，高度动态环境等方面实现传统密码体制、将可追踪溯源与其他技术有机结合起来，以达到安全，轻量级，去中心化和边缘化隐私保护模式，是未来研究的趋势。

3 智能电网中保护隐私的数据查询

3.1 智能电网中保护隐私的数据查询研究

隐私保护技术的发展是随着云计算、物联网技术不断进步的，人们利用云计算、大数据等新兴技术可以更好地为客户提供便捷优质服务。在云计算技术和大数据技术条件下，很多网络公司都是基于用户对各种服务进行分析和预测。但同时也会有个人隐私受到侵害的风险发生。为了防止出现隐私泄露问题，可以利用以下四种方法来对用户和隐私进行保护：第一是针对数据存储进行隔离从而确保隐私不被泄漏。通过将隐私数据存储于安全的数据中心，通过数据访问实现和控制隐私数据处理过程中会存在一定的安全风险。在保护数据隐私方面有四类。其中包括密码和密钥管理安全密钥技术及安全技术如密钥管理技术(ECDC)等[3]。其次，密码技术可以实现物理保护与电子加密相结合实现隐私保护。该技术利用加密技术达到数据不被泄露或被窃取（包括读取、分析或解密）情况下获取隐私数据内容的目的。其次是访问控制安全设计是目前隐私保护领域非常重要的问题之一，也是智能电网发展最快并最为成功技术之一。目前智能电网对于用户数据的保护主要通过以下几种方法：数字签名、数据加密技术、密钥管理、哈希算法、密令解密、数字签名等处理方法来保护通信双方合法用户不被窃

取或者侵犯。针对数据隐私保护有很多方式可供选择，但是安全与隐私保护结合则是研究方向之一。例如：根据公钥计算和加密算法可有效地降低恶意攻击造成数据泄露事件所带来风险及其带来的危害。最后一个是安全访问协议控制方法[4]和访问控制算法两种安全模式（安全和隐私保护）技术为隐私安全提供了有效手段。

3.2 智能电网中保护隐私的数据查询研究相关工作

为满足智能电网系统对设备运行过程中有关用户和电网信息的需求，我国电力行业持续快速发展。目前，已经基本形成了以电网为核心、区域能源互联、高效智能运行服务的新模式。随着科学技术不断发展，电气网络也变得越来越复杂。基于物联网设备的连接使得我们能够实时地获得电力资源所需要的各类信息（如地理位置、距离等）。这对于数据采集系统是至关重要，因为它可以提供一种快速而准确地获取信息并进行分析。传统电力系统一般是根据用户所需自动生成供电计划和调度安排表以及相关的用电信息表，这些用电信息对于企业或者个人来说只能通过查看了解。但是在目前信息化技术环境下，人们可以通过访问自己设备获取到更多信息。智能电网中包括了大量与能源有关的数据和应用程序。该数据对智能电网建设很重要，但是如果保护隐私则会造成严重伤害。

3.3 隐私保护与共享研究未来发展趋势

智能变电站可以采集到大量的能源数据，比如：用户用电信息、电表电量、地理位置、故障信息等。这些数据对于保障电网安全运行具有重要意义。同时，还可以根据智能电网相关系统提供各种辅助决策指标、电量统计、故障预测、在线监测、用电管理等。这些数据可以为电网人员工作和决策提供大量的辅助依据和支持。并且可以根据这些数据调整电力系统。所以该领域的相关数据需要安全隐私保护技术才能保证其合法和有效运作。智能变电站系统在整个工业生产中扮演着非常重要的角色，它可以提高生产效率并且为生产带来价值。当将大数据应用到智能电网时可以更好地分析各种信息并进行准确地决策。该技术将会为智能电网更好地提供能源以及环境保护等各方面服务提供有力基础。智能电网包含了大量电网建设数据和服务应用程序，其中包括用户所需要使用与电网相关的电力数据和相关应用程序。由于涉及到众多信息（如用电类型、电价、地理位置等),智能变电站也将被部署到各类环境下开展工作并收集大量相关数据信息，这些应用程序和数据为进一步了解电网现状提供了更多可能性。这些数据与通信设备或者智能电网相关设备与电力系统发生冲突时会出现这些情形：如果数据泄露将会给整个社会带来危害甚至造成人身伤害。因此保护个人信息非常重要。但是，如果这些数据被侵犯那么它就可能对智能电网带来严重损害，所以必须予以保护[1]。通过保护隐私则可以使整个能源网络安全并让电网更加高效地运行维护人们生活水平以及社会经济效率更加美好。智能变电站是智能电网中重要组成部分，它是通过网络将各类设备连接起来为电力系统提供辅助服务并进行有效控制和管理。因此具有很大商业价值和发展前景，并且随着智能电网的建设与发展，智能变电站会变得越来越智能、越来越完善，因为智能电网会不断发展给电网运行带来新挑战并且也会产生更多新问题；因此需要对智能变电站进行更深入地分析和研究[2]。

4 相关实例

4.1 密码学技术相关实例

为了保护智能电网中的隐私，我们需要在不同的角色之间建立一种安全方式的双向通信。如果用户无法成功地访问自己的智能电网相关数据，则无法直接了解系统本身并且不能在未来提供相应支持及帮助。例如，在一些智能电网技术中，不同类型用户对于不同角色都有一定要求，比如身份验证等等。目前，安全计算技术发展起来之后如何实现这些访问是非常困难的。如果想要解决这些问题则需要了解用户及其设备当前的状态、当前可用信息以及相关属性来确定该用户是否是合适的角色。在多角色访问中有两种方式：身份认证以及数据存储访问。而大多数身份认证系统中主要用于提供给不同角色登录方法并在其注册信息中填写相关信息。我们可以对登录方式进行改进以增强安全计算体验。对于有身份认证权限的用户可以通过“一串密钥”实现身份验证以及访问控制。通过该过程，我们可以对一个用户使用某个设备时所产生的每一个数据集合进行加密处理以保护其隐私，并且由于这种加密方式而无法使用网络中的其他任何信息。此外，如果不能访问该数据会对系统安全带来威胁并产生严重后果。我们可以将其定义为用户/终端设备之间安全以及密钥解密操作在相互通信过程中受到严格

保护的私密部分以及信息加密措施，也就是通过使用解密工具获取私密信息的方法或技术应用时所使用至安全密钥等相关信息时也需要进行有效控制。这些数据能够得到有效地利用和保护也是在确保隐私方面非常重要的一环。因此对于这些用户可以拥有一份密钥而不对其进行访问以防止其被他人访问到或者知道整个信息数据。目前一般采用安全加密技术以及数据管理系统来帮助制定基于规则应用程序中实现身份验证以及数据存储访问控制要求。该方案首先是将整个身份验证机制应用于用户身份管理中并将对其进行认证等工作，同时可以保护用户隐私不被侵犯及知道该信息并以此来提升系统安全性能。

4.2 网络模拟环境

在智能电网中，通信重要组成部分，安全防护也是通信的重要保障。这就要求保护通信环境不被黑客侵入，不会有恶意行为，也不会泄露私人信息。在未来的智能电网中使用移动互联设备，这些设备可以快速、准确地提供各种应用程序，如远程控制系统、电力网络以及其他能源应用。例如电力传输控制系统、计量系统以及其他能源相关业务。通过建立网络对这些设备进行远程操作或者访问还可以通过移动互联网进行通信。为了有效地保护数据隐私也是需要采用网络安全审计技术和方案来保证信息安全和隐私得到保护。安全审计可分为硬件安全审计和软件安全审计，等。其中硬件安全审计通常用来检测和判断计算机中的应用程序是否有后门或攻击等安全威胁，并有效地保护应用程序免受攻击或者威胁。安全审计主要包括行为审计和系统运行审计。为了提高安全设备保护方案和手段，还需要进行安全监控分析等工作，这也是智能电网安全体系架构所要解决的核心问题之一。

4.3 隐私保护相关实例

为了满足电网数据传输需求安全防范工作也应做好相应准备。需要考虑到隐私保护问题，同时为了保障通信安全而选择安全保密方案是最佳选择。这些算法在通信过程中不需要额外透露任何用户信息或者数据（如设备编号),从而能够有效地避免隐私泄露带来威胁。同时也能够保证通信数据具有真实性和完整性。为保证安全计算环境下数据访问行为符合保密要求，隐私环境不会被外界窥探并利用来防止泄露隐私信息。同时设备与计算机之间可以进行双向通信以及远程控制等。因此必须要对网络安全防护技术进行必要研究设计和分析控制来保护相关应用程序等。

5 小结

智能电网技术不断发展，技术水平不断提高，它不仅改变了人们生活、生产、消费方式，还成为能源革命的核心技术之一，对能源行业、经济和社会发展都产生了巨大影响，已成为全球能源发展战略性和基础性战略性产业之一。目前，我国的电力行业已经形成了以电力装备制造为核心、多能互补与综合利用、高效清洁的新型能源结构。这为我国电力行业提供了有力支撑和保障，同时也成为了世界上最具活力以及创新能力最强的能源行业之一。为促进能源可持续利用方式转变提供有力保障。智能电网技术的快速发展有利于优化能源结构并且可以推动传统电力行业向高效、可持续、智能方向发展，为应对新技术对能源安全和电网发展带来的影响，本文主要介绍了智能电网中安全隐私保护和数据查询分析方面研究相关工作以及目前存在问题与发展趋势等工作。

参考文献

[1] 徐淑华. 面向智能电网的隐私保护数据聚合方案研究[D].浙江工商大学,2022.

[2] 李坤昌,石润华,李恩.智能电网中数据聚合与用户查询隐私保护研究[J].信息网络安全,2021,21(11):65-74.

[3] 盖娜. 智能电网中基于本地差分隐私的隐私保护数据聚合机制研究[D].中国科学技术大学,2021.

[4] 李晨阳. 智能电网环境下的隐私保护技术研究与实现[D].北京邮电大学,2020.

[5] 张轩溢. 智能电网中隐私保护数据聚合研究[D].长安大学,2020.

[6] 周华. 智能电网中用户多维数据聚合研究[D].西安电子科技大学,2017.