文章编号：2095-4980(2025)05-0429-05

云边协同的智能电网数据安全共享方案

籍勇亮[1]，李松浓[2]，黄宏程[3]

(1.国网重庆市电力公司，重庆 400015；2.国网重庆市电力公司 电力科学研究院，重庆 401123；
3.重庆邮电大学 通信与信息工程学院，重庆 400065)

摘　要：近年来，智能终端和无线网络的快速发展使电力物联网终端设备和数据量呈指数级增长。这些数据资源已成为电力企业的重要资产，能够显著提升电网的智能感知、内控能力和客户服务效率。但作为国家关键基础设施的核心要素，电力数据极易成为网络攻击目标，一旦泄露会带来重大安全风险和经济损失。因此，电力企业需加强数据安全防护，解决数据交换共享和数据挖掘中的安全问题。本文提出一种云边协同的智能电网数据安全共享方案，通过结合零知识证明技术与秘密共享方案，实现细粒度访问控制和用户访问需求隐私保护。仿真结果表明，本文进行分布式数据访问验证所需时间不超过48 ms，该算法具有较好的性能。

关键词：数据共享；隐私保护；细粒度访问控制

中图分类号：TP393.0　　**文献标志码：**A　　**DOI：**10.11805/TKYDA2024382

A cloud edge collaborative smart grid data security sharing scheme

JI Yongliang[1]，LI Songnong[2]，HUANG Hongcheng[3]

(1.State Grid Chongqing Electric Power Company，Chongqing 400015，China；2.State Grid Chongqing Electric Power Research Institute，Chongqing 401123，China；3.School of Communication and Information Engineering，Chongqing University of Posts and Telecommunications，Chongqing 400065，China)

Abstract：In recent years，the rapid development of smart terminals and wireless networks has led to an exponential growth in the number of terminal devices and data volumes in the power IoT. These data resources have become important assets for power enterprises，significantly enhancing the smart sensing，internal control capabilities，and customer service efficiency of the power grid. However，as critical national infrastructure，power data is vulnerable to cyber-attacks and theft. If leaked，it could cause significant security risks and economic losses. Therefore，power enterprises must strengthen data security protection to address the security issues in data exchange，sharing，and mining. A cloud-edge collaborative intelligent grid data security sharing scheme is proposed，combining zero-knowledge proof technology with a secret sharing scheme to achieve fine-grained access control and privacy protection for user access requests. Finally，the simulation results show that the total time required to perform distributed data access verification in this paper is no more than 48 ms，indicating that the algorithm has a good performance.

Keywords：data sharing；privacy protection；fine-grained access control

近年来，随着智能终端和无线网络的快速发展，连接到电力物联网的终端设备和数据量呈指数级增长[1-2]。大规模物联网设备的集中接入，促使电网运行过程中生成并沉淀了高价值数据资源。这些资源已成为企业的核心资产，充分挖掘这些数据资产的价值，可大大促进电网智能感知、内控能力和客户服务效率的提升；电网调度运行数据共享也能为电力生产、营销等带来便利。

收稿日期：2024-08-15；**修回日期：**2024-09-24

基金项目：重庆市自然科学基金资助项目(面上项目)(2024NSCQ-MSX1283)；国网重庆市电力公司科技资助项目(52202324001D)

引用格式：籍勇亮,李松浓,黄宏程. 云边协同的智能电网数据安全共享方案[J]. 太赫兹科学与电子信息学报, 2025,23(5):429-433. DOI:10.11805/TKYDA2024382.

Citation format：JI Yongliang,LI Songnong,HUANG Hongcheng. A cloud edge collaborative smart grid data security sharing scheme[J]. Journal of Terahertz Science and Electronic Information Technology, 2025,23(5):429-433. DOI:10.11805/TKYDA2024382.

电力数据作为国家关键基础设施的核心要素，事关国家安全，很容易成为网络攻击和窃取的目标，这些业务数据一旦丢失、损坏或泄露，可能引发电力系统故障或重大安全事件，给国家和企业带来巨大的经济损失[3]。因此，电力企业必须加强电力敏感数据资产的安全防护，解决好价值数据交换共享、数据挖掘等安全问题。电网数据通常通过云计算实现海量数据的存储和分析处理，目前大多数企业也主要采用基于云的数据共享方式，但这种方式存在数据泄露、访问控制和单点故障等问题[4−6]。此外，电力数据共享方面，相关用户访问和共享电网数据首先需要解决身份合法性的问题；同时电网数据自身的敏感性使其往往需要实施分级分类管理，而用户权限的差异性意味着能够访问的数据级别不同，传统访问控制方案难以满足敏感电网数据[7−8]的动态防护需求。

为解决上述问题，本文提出一种云边协同的智能电网数据安全共享方案。将零知识证明技术[9]与秘密共享方案[10]结合起来，实现智能电网中数据的细粒度访问和用户访问需求隐私保护。首先引入云边协同架构，边缘服务器存储合法用户的数据访问凭证，通过多个边缘服务器协同对用户完成数据访问前的权限认证。然后，用户通过零知识证明协议在不暴露访问需求的情况下完成认证。最后，通过秘密共享方案将验证过程扩展至多个边缘节点中，避免单点故障。

1 系统模型

本方案的系统模型如图 1 所示，主要由以下几部分组成：

公钥生成中心(Key Generation Center，KGC)：KGC 是可信的第三方机构，主要用于生成零知识证明和秘密共享的安全参数，并分发公钥至云服务器(Cloud Server，CS)，私钥至用户。公钥用于验证用户的私钥，以判断用户是否拥有相关数据的访问权限。

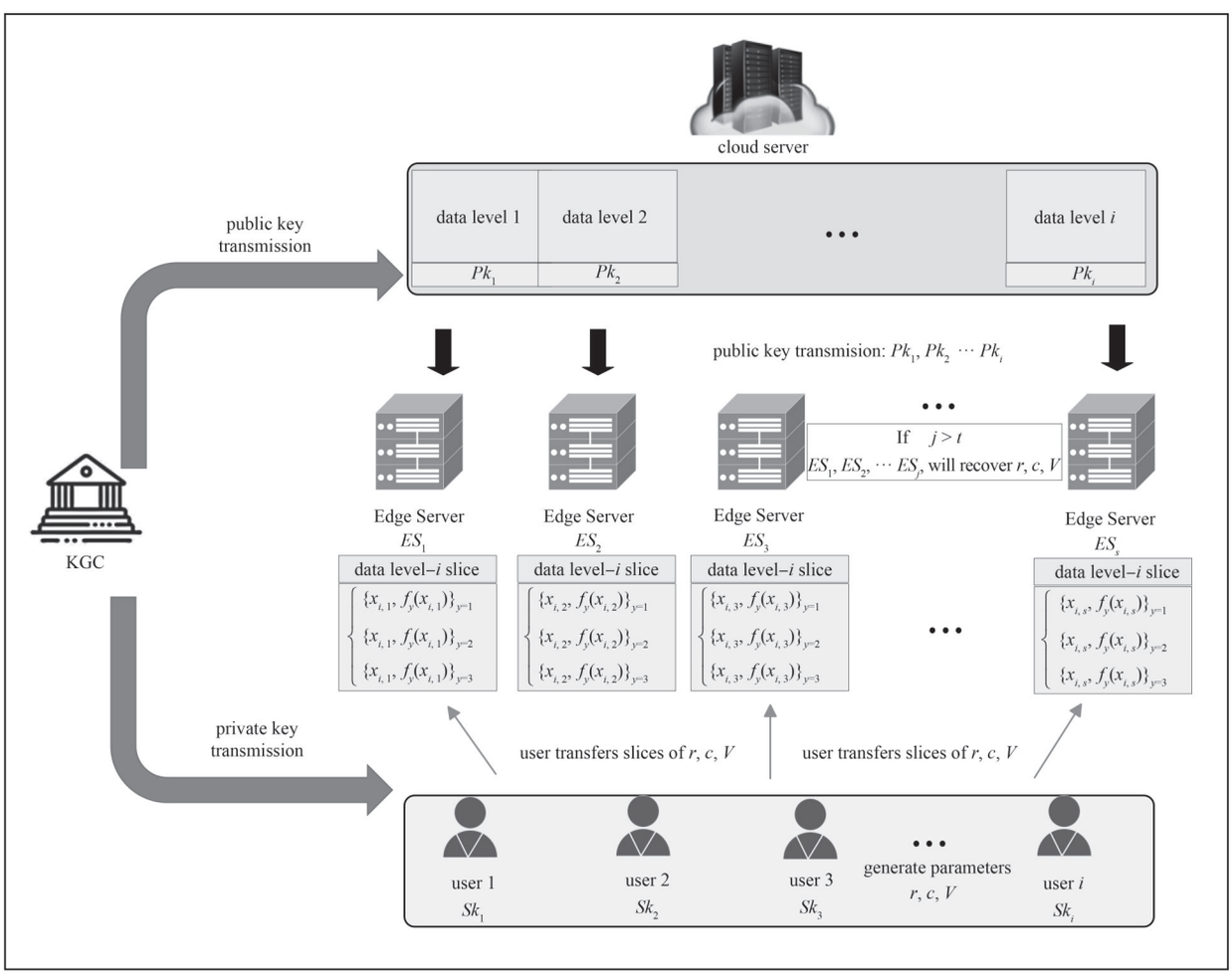

Fig.1 System model

图 1 系统模型

云服务器(CS)：云服务器拥有强大的计算能力和存储能力，主要负责保存由终端物联网设备上传的电力数

据。电力数据由相应标准分级分类，形成不同的数据库。云服务器将不同的数据与相应的公钥建立对应关系，形成电力数据列表。云服务器分发公钥至分布式边缘节点，边缘节点可凭借公钥对用户进行验证。

边缘服务器(Edge Server，ES)：ES负责用户的合法性验证与权限确认，通过多个ES的协同验证避免验证过程被攻击者操纵，危害数据共享系统的安全性。

访问用户(Access User，AU)：AU对电网中的数据有访问需求时，根据不同的用户权限级别访问分类分级的电网数据。为保护用户的隐私，用户对特定数据的访问需求在验证过程予以保护。具有访问需求的用户将通过自身接收的私钥向边缘节点发起验证。由于边缘服务器具有分布式架构，用户会将验证所需的参数通过秘密分享算法进行切片，最后由多个边缘节点联合进行参数恢复并进行验证。

2　方案设计

2.1 总述

为不同AU能够共享智能电网中的数据，且相应AU能够划分对应的数据访问权限。本文首先将不同类别的数据与特定的公钥建立对应关系，生成电力数据列表存储在CS中。然后，通过KGC颁发给AU的私钥进行用户权限的验证。为防止CS进行验证时可能导致的单点故障、隐私泄露等问题，通过云边协同的方式将AU的验证过程扩展到多ES中，分布式的ES可以协同认证。

本文设计了秘密共享方案，将AU验证所需的各种凭证通过切片的方式分发至多个ES中，只有满足特定数量的ES共同计算，才能完成验证过程。此外，由于AU的私钥与数据列表中的公钥具有对应关系，为不暴露用户具体访问需求，本文通过零知识证明方案在不暴露AU私钥的情况下证明AU拥有相应数据公钥的对应私钥。

2.2 系统建立

1) 全局参数生成。KGC首先生成零知识证明需要的公共参数。设$E(F_p)$为有限域F_p上的椭圆曲线，其中p为一个大素数；G为曲线上的基点，作为n阶子群的生成元。全局参数由电网系统中的各个实体共享。KGC为AU生成私钥sk，sk从$[1,n-1]$中随机选取；然后通过椭圆曲线点乘生成公钥$Pk=G\cdot[sk]$。用户保存sk，作为能够访问相应数据的凭证。

2) 电力数据列表。KGC将AU_i对应的公钥Pk_i分发至CS。CS根据用户的权限级别将Pk_i与对应数据建立关联，生成电力数据列表，如数据种类$D_i \leftarrow Pk_i(sk_i)$

2.3 非交互式零知识证明权限认证

1) AU权限认证参数生成。AU_i从$[1,n-1]$选择随机数v，并通过点乘生成$V=G\cdot[v]$。然后，AU_i生成公共验证凭证$r=v-sk_i\times c$。其中$c=H(G\|V\|Pk_i)$，H为哈希函数。

2) 验证方权限认证。当检验AU_i合法性的验证方接收到r、c、V后，进行合法性认证。验证方主要监测AU_i是否拥有相应数据库公钥Pk_i对应的私钥sk_i，但不知道sk_i具体数值。因此验证方首先根据自身拥有的公钥Pk_i、G和接收的V验证c，确保Pk_i是有效的公钥。然后通过式(1)进行认证：

$$r\cdot[G]\stackrel{?}{=}V-Pk_i\times c \tag{1}$$

若式(1)成立，则验证方可以判断AU_i拥有相应的私钥。

2.4 云边协同的多节点协同认证

为执行多ES的分布式认证，AU_i首先需将权限认证参数r、c、V通过秘密分享进行切片。假设边缘服务器集合为$E=\{e_1,e_2,\cdots,e_s\}$，s为边缘服务器数量。选取秘密恢复阈值为$2\leqslant t\leqslant s$，t为秘密共享恢复所需的最少节点数量。

1) 秘密切片生成。用户AU_i选择一个大质数p且$u_{\text{secret}}<p$，u_{secret}表示AU_i需要切片的秘密值。然后，AU_i随机生成$t-1$个随机数a_i，r、c、V分别作为常数项构造秘密共享多项式：

$$\begin{cases} f_1(x)=a_{t-1}x^{t-1}+\cdots+a_2x^2+a_1x+r \\ f_2(x)=a_{t-1}x^{t-1}+\cdots+a_2x^2+a_1x+c \\ f_3(x)=a_{t-1}x^{t-1}+\cdots+a_2x^2+a_1x+V \end{cases} \tag{2}$$

AU_i随机生成s个非零数$x_{i,k}(1\leqslant k\leqslant s)$代入多项式$f_y(x),y=1,2,3$，得到$\{x_{i,k},f_y(x_{i,k})\}$，分发给$s$个ES。因此每个

ES 可获得 3 份秘密份额：$\{x_{i,k}, f_y(x_{i,k})\}_{y=1}$、$\{x_{i,k}, f_y(x_{i,k})\}_{y=2}$、$\{x_{i,k}, f_y(x_{i,k})\}_{y=3}$。

2) 秘密恢复。对于 s 个 ES，其中的 t 个及以上 ES 可协同恢复 r、c、V。每个 ES 互相转发自身携带的 3 份秘密份额，当接收的每类秘密份额大于等于 t 时，可通过式(3)进行恢复：

$$f(u_{\text{secret}},x)=\sum_{k=1}^{t}\left(f(x_{i,k})\times\prod_{j=1,j\neq k}^{t}\frac{x-x_{i,j}}{x_{i,k}-x_{i,j}}\right)(\text{mod}\,p) \tag{3}$$

一旦得到 $f(u_{\text{secret}},x)$，ES 可以代入 $x=0$ 恢复出秘密，即得到 r、c、V。

3) 云边协同认证。CS 首先将电力数据列表中的公钥分发给参与秘密恢复的 ES。此时每个 ES 拥有 AU_i 发送的权限认证参数 r、c、V 与公钥列表，它们通过式(1)验证用户 AU_i 的访问权限，随后根据其验证结果进行投票机制，若其中超过半数的 ES 认定，则权限认证通过。

3 安全分析

1) 细粒度访问控制。由于电网数据分级分类的制度以及电力数据自身所具有的敏感性，用户拥有不同的权限级别，具有对符合自身权限的数据访问权。本文中，与特定数据库相关联的公钥和用户私钥由 KGC 计算并分发给云服务器和用户。云服务器根据用户的权限将对应的公钥与符合该级别的数据库关联。因此，用户通过私钥进行访问时，边缘服务器只能找到符合对应公钥的数据库。

2) 权限认证安全性。用户进行数据访问时，需要证明自身拥有相应数据库的私钥，但不能向边缘服务器展示私钥的真实内容。本文通过椭圆曲线离散对数问题的数学困难性确保验证过程的安全性，使边缘服务器无法从公钥推断出对应的私钥。

3) 分布式认证安全性。由于单一验证者在进行用户合法性认证时容易遭受攻击，导致单点故障问题。本文将用户的合法性认证扩展到多个边缘服务器中，通过秘密共享机制，保证大于特定数量的服务器可进行协同认证，容忍一定数量的恶意边缘服务器存在。

4 仿真分析

使用 Python3.9 计算机进行仿真实验，CPU 为 AMD Ryzen 9 8945HS、4.00 GHz，内存为 32 GB。仿真参数设置为：边缘服务器数量为 100、200、300；秘密恢复的阈值为 10、40、70；密钥长度设为 128、512、1 024。

1) 评估不同边缘服务器数量、不同阀值下的秘密共享算法性能，结果如图 2 所示。由图 2 可知，秘密恢复时间最高不超过 22 ms。在相同数量的边缘服务器下，阈值越高，所花费的秘密恢复时间越多。这是因为参与恢复的边缘节点数量增加了；在相同阈值下，边缘服务器数量越多，所花费的秘密恢复时间也越多。这是因为边缘服务器数量增多，用户需分发的秘密切片也相应增加；同时，恢复秘密的阈值设为 10~70，验证了方案的可扩展性。

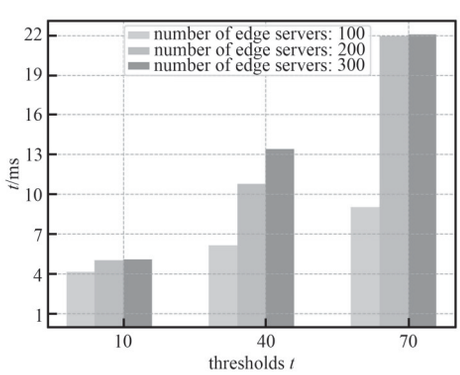

Fig.2 Secret recovery efficiency
图2 秘密恢复效率

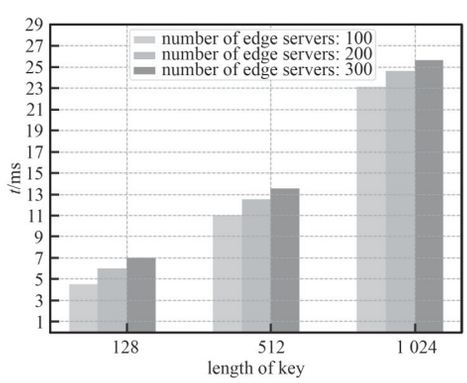

Fig.3 Duration of permission verification
图3 权限验证时间

2) 验证不同数量的边缘服务器、不同密钥安全长度下用户权限验证时间。用户发起访问到完成验证所花费的时间见图 3，由图 3 可知，验证时间不超过 26 ms。随着边缘服务器的增加，用户需分发的秘密份额增加，导致时间增加。此外，零知识证明密钥长度代表不同程度的安全级别，密钥长度越长，所花费的时间也相应更多。

5　结论

本文针对智能电网数据提出了一种隐私保护的细粒度访问方案。通过零知识证明方案保证用户的合法性，并暴露用户的私钥和具体访问需求；通过云边协作的方式将权限认证扩展至多个边缘服务器节点，避免了单点故障问题。在多个边缘服务器协同验证时，将秘密分享与零知识证明相结合，实现多个节点间的协同认证，并对边缘服务器隐藏访问需求。仿真结果表明，秘密恢复时间最高不超过 22 ms，而验证时间不超过 26 ms，表明所提方案具有较好的效率。

参考文献：

[1] 招景明,张捷,宋鹏,等. 一种高效的基于云边端协同的电力数据采集系统[J]. 电网与清洁能源, 2022,38(5):49–55. (ZHAO Jingming, ZHANG Jie, SONG Peng, et al. An efficient method of electric power data acquisition system based on cloud edge collaboration[J]. Advances of Power System & Hydroelectric Engineering, 2022,38(5):49–55.) DOI:10.3969/j.issn.1674–3814.2022.05.007.

[2] 郝旭龙,董国芳. 基于联盟链和属性加密的智能电网数据共享方案[J]. 云南民族大学学报(自然科学版), 2023,32(3):352–358. (HAO Xulong,DONG Guofang. Smart grid data sharing scheme based on consortium blockchain and attribute encryption[J]. Journal of Yunnan University of Nationalities(Natural Sciences Edition), 2023,32(3):352–358.) DOI:10.3969/j.issn.1672–8513.2023.03.012.

[3] 郭少勇,刘岩,邵苏杰,等. 新型电力系统数据跨域流通泛安全边界防护技术[J]. 电力系统自动化, 2024,48(6):96–111. (GUO Shaoyong,LIU Yan,SHAO Sujie,et al. Ubiquitous security boundary protection technology for cross–domain data circulation in new power system[J]. Automation of Electric Power Systems, 2024,48(6):96–111.) DOI:10.7500/AEPS20230629001.

[4] LUO Xinyi, XUE Kaiping, XU Jie, et al. Blockchain based secure data aggregation and distributed power dispatching for microgrids[J]. IEEE Transactions on Smart Grid, 2021,12(6):5268–5279. DOI:10.1109/TSG.2021.3099347.

[5] KIM Y,HAKAK S,GHORBANI A. Smart grid security:attacks and defence techniques[J]. IET Smart Grid, 2023,6(2):103–123. DOI:10.1049/stg2.12090.

[6] 左建业. 智能电网中面向隐私保护的数据聚合算法[J]. 太赫兹科学与电子信息学报, 2021,19(3):485–489. (ZUO Jianye. A privacy–preserving data aggregation algorithm in smart grid networks[J]. Journal of Terahertz Science and Electronic Information Technology, 2021,19(3):485–489.) DOI:10.11805/TKYDA2019368.

[7] DONG Yu, SHAN Xin, YAN Yaqin, et al. Architecture, key technologies and applications of load dispatching in China power grid[J]. Journal of Modern Power Systems and Clean Energy, 2022,10(2):316–327. DOI:10.35833/MPCE.2021.000685.

[8] WANG Yuntao,SU Zhou,ZHANG Ning,et al. SPDS: a secure and auditable private data sharing scheme for smart grid based on blockchain[J]. IEEE Transactions on Industrial Informatics, 2021,17(11):7688–7699. DOI:10.1109/TII.2020.3040171.

[9] SUN X Q,YU F R,ZHANG P,et al. A survey on zero–knowledge proof in blockchain[J]. IEEE Network, 2021,35(4):198–205. DOI:10.1109/MNET.011.2000473.

[10] ZHANG E,LI M,YIU S M,et al. Fair hierarchical secret sharing scheme based on smart contract[J]. Information Sciences, 2021(546):166–176. DOI:10.1016/j.ins.2020.07.032.

作者简介：

籍勇亮(1979–)，男，博士，高级工程师，主要研究方向为电工理论新技术、输变电运维技术. email: 33525765@qq.com.

李松浓(1980–)，男，博士，正高级工程师，主要研究方向为智能电力传感器技术、能源量测技术、电力系统通信技术.

黄宏程(1979–)，男，博士，教授，博士生导师，主要研究方向为边缘计算、网络安全、新型电力系统、人机智能交互技术.