分 类 号： TP391

学校代码： 10109

密　　级： 公 开

太原科技大学硕士学位论文

（学术型）

学位论文题目：基于联邦学习的智能电网负荷预测研究

英 文 题 目： **Load Forecasting of Smart Grid based on Federated Learning**

研 究 生 姓 名 ： 曲晓东

导师姓名及职称： 谢刚　教授

培　养　单　位： 电子信息工程学院

学　科　专　业： 控制科学与工程

论文提交日期： 2023 年 4 月

论文答辩日期： 2023 年 6 月 4 日

答辩委员会主席： 阎高伟　教授

中国知网　https://www.cnki.net

中 文 摘 要

随着智能电网的不断普及和高级量测体系的建立，智能电网中产生了海量的用电数据。这些数据可以有效的帮助电力公司对电网中的负荷进行有效预测。准确安全的负荷预测对于电力生产、输电和维护至关重要。当前深度学习模型已经取代其他经典模型成为最流行的预测模型。但深度预测模型需要用户提供大量的私人用电量数据，这一行为存在潜在的隐私泄露风险。边缘节点可以使用联邦学习通过聚合对全局模型进行联邦训练。作为一种新型的分布式机器学习技术，联邦学习只发送模型参数，不共享原始数据。然而，现有的基于联邦学习的预测方法仍然面临着数据异质性、隐私泄露和通信瓶颈的挑战。针对这些问题，本文进一步改进基于联邦学习的负荷预测方法，提出了基于个性化联邦学习的负荷预测方法和基于单次联邦学习的高效负荷预测方法来解决相应问题。主要工作内容有：

（1）提出了一个基于个性化联邦学习（PFL）的用户级负荷预测方法。该方法训练出的个性化模型在本地数据的预测表现上要优于全局模型。此外，我们在该方法中引入了一种新型差分隐私算法来提供额外的隐私保障。该算法基于生成对抗网络原理，在整个博弈过程中实现了隐私保证和预测精度之间的平衡。我们在真实数据集上进行了仿真实验，实验结果表明，该方法能够满足实际负荷预测场景对准确性和隐私性的要求。

（2）针对联邦学习的通信瓶颈问题，我们设计了一种基于单次联邦学习（one-shot FL）的高效负荷预测方法。该方法针对于负荷预测中的客户端数据 non-IID 的场景，利用蒸馏数据的传输来完成客户端与服务器之间的单次通信，最终在蒸馏数据上进行全局模型训练，完成用户负荷预测任务。在大幅降低通信成本的同时，该联邦学习框架使用蒸馏数据来代替梯度进行传输，避免了由梯度泄露反推私人数据集的可能，提升了该方法的隐私保护性能。

关键词：智能电网；负荷预测；联邦学习；个性化联邦学习；数据集蒸馏

中国知网 https://www.cnki.net

ABSTRACT

With the rapid development of smart grids and the extensive deployment of advanced metering infrastructure, massive electricity consumption data is generated in smart grid. These data can help power companies effectively forecast the load in the grid. Accurate and safe load forecasting is essential for power production, transmission, and maintenance. At present, the deep learning model has replaced other classical models as the most popular prediction model. However, the deep prediction model requires users to provide a large amount of personal power consumption data, which has potential privacy leakage risks. Edge nodes can federally train global models through aggregation using federated learning (FL) As a new distributed machine learning technique, FL only sends model parameters and does not share raw data. However, existing FL-based forecasting methods still face the challenges of data heterogeneity, privacy disclosure, and communication bottlenecks. To solve these problems, this paper further improves the FL-based load forecasting algorithm and proposes a load forecasting framework based on personalized federated learning and a high-efficiency load forecasting framework based on one-shot federated learning. The main work contents include:

(1) A user-level load forecasting framework based on personalized Federated Learning (PFL) is proposed. The personalized model trained by this framework outperforms the global model on local data. In addition, we introduce a novel differential privacy algorithm in the proposed system to provide an additional privacy guarantee. Based on the principle of generative adversarial network, the algorithm achieves the balance between privacy and prediction accuracy throughout the game. We perform simulation experiments on the real-world dataset and the experimental results show that the proposed system can comply with the requirement for accuracy and privacy in real load forecasting scenarios.

(2) To address the communication bottleneck problem of FL, we design an efficient load forecasting framework based on one-shot FL. This framework aims at the non-IID client data in the load forecasting scenario, using the transmission

中国知网 https://www.cnki.net

of distilled data to complete a single communication between the client and the server, and ultimately conducting global model training on the distilled data to complete the user load forecasting task. While greatly reducing the communication cost, the proposed framework uses distilled data instead of gradients for transmission, which does not involve the update transmission of the model generated during the whole training process. It avoids the possibility of inferring private datasets by gradient leakage, thus greatly improving the privacy protection performance on the client side.

Keywords: Smart grid; Load forecasting; Federated learning; Personalized federated learning; Dataset distillation

中国知网 https://www.cnki.net

目 录

中国知网 https://www.cnki.net

中国知网 https://www.cnki.net

第一章 绪论

1.1 课题研究背景及意义

进入 21 世纪，随着国民经济与科学技术的高速发展，我国对电力资源的需求量呈现持续增加的趋势。2023 年 1 月 16 日，中国国家能源局公布了 2022 年全社会用电量等数据[1]。全社会用电量在 2022 年全年达至 86372 亿千瓦时，同比增长 3.6%。城乡居民生活用电量相比去年也有了较大水平的提升，同比增长 13.8%，达到了 13366 亿千瓦时。无独有偶，有调查表明，美国在过去 20 年的时间里电力需求都在以每年 2.5%的速率逐年上涨[2]，传统电网开始无法有效应对急剧增加的电力需求。此外，全球能源需求日益增加，随之引发温室气体排放量明显上涨，使得加强环境保护、解决全球气候变暖等问题受到国际社会的极大关注[3]。在 2020 年 9 月 22 日举办的第七十五届联合国大会上，中国国家主席习近平提出了“碳达峰、碳中和”的双碳目标[4]，这是中国在全球气候变化新形势下向全世界做出的庄严承诺，促使我国能源产业向绿色低碳快速转型。为了满足电力产业的高质量发展要求，人们开始着手于清洁、低碳、安全、高效的能源体系建设，智能电网应运而生，并在过去的十几年里开始迅速普及。

智能电网（Smart Grid，SG），也被称为未来电网、互联电网、电网智能化[5]，是在 20 世纪电网基础上进行的改进。传统电网一般仅限于能源传输，将电力从发电机输送到大量用电客户。相比之下，借助于电力和信息的双向传输，智能电网创立了一个具有自动化和分布式特点的高级电力输送网络。按照中国电力科学研究院的介绍[6]，智能电网是以传统物理电网为基础，将当前发展成熟的传感测量技术、控制技术、信息技术、通讯技术和计算机技术与物理电网高度集成而形成的新型电力网络。利用现代信息技术，智能电网可以用更有效的方式提供电力，优化资源配置，同时对发电、输电、配电和用电中发生的各种情况和事件做出及时反应，并采取相应的策略，比如故障处理和负载调整。智能电网确保了电力供给的安全性、可靠性和经济性，满足了能源网络的环保约束，实现了为用户提供可靠、经济、清洁、互动的电力供应和相关服务的目标。

电力不能作为一种特殊的商品储存，因此保证电力供需平衡对电力系统的稳定至关重要。在这一背景下，电力系统负荷预测作为基础支撑工作，对我国新能源事业的发展和产能结构的转型升级具有重要意义。近年来，由于高级量测体系（Advanced Metering Infrastructure，AMI）的大量部署以及通信水平的迅速提升，电网公司的用电信息采集系统积累了海量异构负荷数据，为人工智能、大数据分析等前沿技术在电力系统负荷预测领域的应用提供了重要数据基础[7]。同时，人工智能、大数据分析等数字化技术发展迅

中国知网 https://www.cnki.net

速，已经在计算机视觉等研究领域取得了不错成果，从而为电力系统负荷预测研究提供了新手段和关键技术支撑[8]。然而，一些安全和隐私问题阻碍了负荷预测模型的后续研究和应用。

人们认为不合理和不安全的数据应用是对数据安全和隐私保护的重要挑战。智能电表是 AMI 的核心，它记录住宅能源消耗，并定期将这些数据上传到能源供应商。智能电表数据反映了用户的个人用电习惯，如被滥用极易侵犯用户隐私。因此，考虑到数据安全和个人隐私问题，消费者普遍反对安装智能电表[9]。参考欧盟通用数据保护条例（General Data Protection Regulation，GDPR），客户用电数据的收集或存储也受到数据最小化原则和同意原则的严格限制。此外，随着智能电网的快速发展，收集自智能电表的用电负荷数据规模正在以前所未有的速度增长。传统的集中式模型训练受到通信和计算能力的限制，难以收集和存储海量数据[10]。而且，当 AMI 用于传输用户用电数据时，这些用户负荷数据也会面临数据盗窃[11]、数据篡改[12]和虚假数据注入[13]等恶意行为。同时由于用户用电习惯不同所带来的数据异构性问题也会使得预测模型的收敛速度和准确性表现较差。因此，构建一个具有个性化、隐私性和鲁棒性的用户用电负荷预测系统对构建“清洁低碳、安全高效”的现代能源产业体系具有重要意义。

1.2 国内外研究现状

电力系统负荷预测是根据历史电力负荷数据作为预测支撑，建立数学模型，寻找负荷与其他相关因素（如时间、天气、经济）的内在关联，实现对电力负荷精准预测。电力负荷的准确预测不仅能保障电力系统的正常运行，还可以大大减少资源消耗。通常电力系统负荷预测任务往往以预测所用的时间周期[14]来作为分类依据。具体来讲，短期预测属于时分预测、日度预测，用于在线监控电力设备的日常运行和降低调度成本；中期预测是用于预测周、月、年度负荷，来进行电力业务规划如检修计划；长期预测则是进行多年度预测，对电网未来发展制定规划目标。

负荷预测在许多方面都对电力系统行业具有重要的意义。作为电力系统调度的重要组成部分，负荷预测要准确地给出电力市场上的购电和发电信息，防止能源浪费和滥用。在电力资源调度、可靠性分析和发电机维修规划等方面，也都要求负荷预测具有较高的准确性。然而电力负荷预测是一个复杂的非线性问题，季节差异、气候变化、周末节假日、灾害、电厂运行场景和网络故障等因素都会导致负荷需求随之变化。所以，建立准确安全高效的短期负荷预测模型，对电力公司提前规划用电调度，指导电能价格合理制定，保障电力交易市场的高效经营，提高供电质量，保证居民和工厂等全社会的正常用电具有重要意义[15]。

中国知网 https://www.cnki.net

1.2.1 负荷预测方法

对国内外历年的负荷预测研究成果进行整理，能够发现负荷预测的研究大致经过了两个发展阶段，第一个阶段主要是围绕传统的数学模型进行负荷预测，后续的第二阶段则是基于当前蓬勃发展的人工智能技术来开展研究工作。

谈及经典预测方法，基本上是以时间序列法、回归分析法、灰色预测法[16]这些基于统计学知识的方法为主。时间序列法在电力系统负荷预测中运用较为普遍，需要先将电力负荷历史数据按照时间顺序进行排列，基于这些数据进行数据建模操作，而后在这些建立的模型上预测未来的负荷情况。基于电力负荷的周期特性和时间持续性，时间序列法确定了该负荷序列随时间的基本变化规律，并借此来开展预测任务。在实际应用时间序列法时，往往先将电力负荷序列视为一个时间序列，然后按照不同的变化趋势进一步将其分解为四个分量：周期分量、非周期分量、随机变化分量和季节变化分量[17]。在分解过程中，非周期分量包括电力负荷的自然波动趋势；季节变化分量则表示电力负荷随季节、气候、温度的变化趋势；随机变化分量则涵盖其他因素导致的一些负荷不确定性。虽然时间序列法的预测过程较为简单，涉及的样本和计算量较小，但因局限于样本数据的拟合，未曾对影响负荷变化的其余要素进行考虑。

同时间序列法类似，回归分析法[18]也需要在电力负荷历史数据的基础上进行操作。只是回归分析法在分析历史数据的基础上，也加入了对影响负荷的外在因素的考虑。基于数据统计原理，回归分析法对历史负荷数据进行数学处理，将电力负荷作为因变量，其他影响因素作为自变量，通过建立因变量和自变量间确定的函数关系来描述电力负荷同影响因素之间的关系，后续通过给定的输入来获得相应的输出（即预测负荷）。回归分析法的预测过程简单方便，但是该方法得出的固定函数关系无法真实反映实际的负荷变化，因而应用线性回归模型进行预测的误差相对较高。

灰色预测法[19]是基于模糊控制，运筹学和自动控制理论知识，对一个包含各种不确定因素的复杂系统进行预测的方法。在实际应用中，需要将历史用电负荷序列进行一定处理，经由数据生成的方法处理为有序的数据排列，以此建立灰色模型进行负荷预测。灰色预测法的优点是适用性强，运算方便，不依赖大量数据样本，考虑到的变量因素更为全面；但该预测方法也存在较大缺陷，当电力负荷呈现不规则波动时，表现为样本数据离散程度变大，这会导致负荷预测精度下降。

然而，随着智能电网的快速发展与不断演变，尤其是在新型电力系统的构建中引入了大量的分布式新能源、电动汽车等新元素，电力系统负荷类型呈现多元化趋势。面对如此复杂多变的影响因素，传统负荷预测方法难以精准构建新型电力系统背景下的负荷

中国知网 https://www.cnki.net

模式。大数据和人工智能时代的到来，使得基于人工智能的负荷预测方法开始受到研究人员的关注。基于人工智能的负荷预测方法主要包括支持向量机法、模糊预测法和人工神经网络法[20]。

支持向量机（Support Vector Machine，SVM）是基于数学统计理论的一种机器学习方法，本质上是按监督学习方式对样本数据进行二元分类的线性分类器，该方法的基本原理是在特征（或样本）空间来构建最优平面，保证其与其他类样本距离的最大化。基于结构风险最小化原则，在负荷预测任务中，SVM 算法可以解决小样本情况下的机器学习问题，在非线性数据和高维数据上也有较好的预测表现[21]。但在处理大规模的样本数据时需要训练较长时间，模型的最终预测精度对模型参数的选取也较为依赖。

模糊预测法[22]是一种运用模糊数学理论的负荷预测新技术，通过模糊理论模型以一定规则将负荷变化规律和其他模型信息表示出来，应用模糊集合论对电力负荷进行预测。模糊预测法在负荷预测任务中主要包括模糊聚类法、模糊最大贴近度法和模糊相似优先比法等。模糊预测的方法在实际应用中可以有效应对电力负荷变化的不规律性，但需要提供大规模的历史用电数据才能保证一定的预测精度。

随着人工神经网络（Artificial Neural Networks，ANN）在图像识别、自然语言处理等领域的普遍运用，研究人员发现 ANN 在短期电力负荷预测任务中可以实现更高的预测精度。Khan 等人[23]于 2013 年提出了一种基于递归笛卡尔遗传规则进化的人工神经网络，该神经网络模型可以对电力系统各个季节下的不同负荷模式进行有效预测。2018 年张凤林等人[24]使用信赖域算法对 BP 神经网络参数进行了优化，在新能源负荷预测方面取得了良好效果。

近年来，随着硬件设施计算能力的逐年提高，深度学习（Deep Learning，DL）方法开始在图像分类、目标检测、文本语言处理等领域崭露头角。在智能电网的建设过程中，大量部署的 AMI 可以有效地管理电力使用，同时获得巨量的电力消耗数据。大数据和人工智能技术的出现增加了人们对基于 DL 的负荷预测技术的研究热情。与传统方法相比，基于数据驱动的 DL 模型不再依赖专家经验进行特征选择，使其具有更好的预测表现和更强的自适应能力。考虑到递归神经网络（Recurrent Neural Networks，RNN）在时间序列问题上的良好表现，大家都在致力于使用 RNN 及其变体来解决负荷预测问题。Shi 等人[25]提出了一种基于深度 RNN 的家庭负荷预测模型，克服了传统 DL 方法上存在的过拟合问题。但随着时间间隔增长，RNN 会因梯度消失问题难以学习到远距离信息，进而导致预测模型失效。有鉴于此，Hochreiter 等人[26]所提出的长短时记忆网络（Long-Short Term Memory，LSTM）通过增加遗忘门的设计可以有效解决了长序列训练过程中

中国知网 https://www.cnki.net

普通 RNN 网络面临的梯度消失问题。2017 年，Kong 等人[27]基于 LSTM 开发了一个深度预测模型，用来预测加拿大居民用户的短期负荷。该模型充分考虑了居民活动对负荷变化的影响，并将用电设备的信息作为模型输入，最终有效提高了负荷预测的准确率。2020 年，Alhussein 人等[28]提出了一种称为 CNN-LSTM 的混合模型，该模型同时结合了卷积神经网络（Convolutional Neural Networks，CNN）在特征提取方面的优势和 LSTM 在序列数据处理方面的优势，他们开发的框架在真实数据集上的测试表现要明显优于竞争对手。

1.2.2 负荷预测隐私保护

人工智能作为新一轮科学技术革命和工业转型升级的战略技术之一，已经成为全球大部分国家在新一轮技术竞争中的主攻领域。作为本世纪人工智能浪潮全面兴起的关键驱动力，数据在全球竞争中的经济和战略价值不断增加，数据的安全问题同人工智能技术的安全发展密切相关[29]。当前不当的数据利用严重威胁着公众个人乃至社会的隐私安全，有鉴于此，在法律层面，我国于 2020 年先后出台了《中华人民共和国数据安全法（草案）》和《中华人民共和国个人信息保护法（草案）》等法律法规，填补了我国在个人信息和隐私保护领域的相关立法规定，我国个人隐私保护的法律框架得以初步构建。在技术层面，作为处理数据应用和隐私保护间矛盾的有效手段，隐私保护计算需要在有效保护隐私的前提下对数据价值进行挖掘。隐私保护计算不是单一学科，它涉及多学科多领域的交叉融合，这样一个跨学科技术体系包括联邦学习[30]、差分隐私[31]、安全多方计算[32]和同态加密[33]等隐私增强技术。近来的负荷预测研究开始关注考虑隐私保护的联邦学习（Federated Learning，FL），这里就联邦学习在负荷预测领域的应用展开讨论。

考虑到隐私、效率和延迟问题，将所有数据发送到一个集中的位置进行分析或检测通常不适合工业场景，联邦学习作为一种高效的隐私保护手段应运而生。联邦学习本质是一种分布式机器学习范式，它可以在保持原始数据源不出本地的基础上，通过多客户端的本地训练和客户端同服务器间的参数传递，协同训练出一个全局模型。联邦学习在保证合法合规的前提下完成了模型的训练任务，也有效地保障了大数据交换时的信息安全和个人数据隐私。目前，基于联邦学习的负荷预测研究已经较为成熟，并在不同的研究方向上取得了一定进展。Venkataramanan 等人[34]将 FL 应用于分布式能源预测，在实际电网服务中如负荷波动、负荷缩减等情况下取得了良好的预测效果。用电数据的私有属性也引起了人们对其数据安全性和隐私保护方面的关注。Qureshi 等人[35]论证了对基于 FL 的负荷预测系统使用投毒攻击的可行性。因此，Sun 等人[36]提出了一种基于改进差分隐私算法的 FL 模型，以提高负荷预测系统的隐私保护性能。同时在研究过程中，

中国知网 https://www.cnki.net

研究人员意识到负荷数据分布和负荷模式的多样性可能会影响 FL 创建的单个全局模型的准确性。为了解决这个问题，Gholizadeh 等人[37]提出了一种基于 FL 的消费者聚类技术，该技术能够更好地反映消费者的消费模式。然而以上研究方向都只是研究了单个属性，没有综合考虑到实际负荷预测场景中的隐私性、个性化等这些属性之间的相互影响。

1.3 本文研究内容与章节安排

本文以智能电网中的负荷预测任务为研究对象，针对现有基于联邦学习的负荷预测算法中存在的不足分别从个性化和通信效率以下两个方面展开研究，相应的提出了基于个性化联邦学习的负荷预测方法和基于 one-shot 联邦学习的高效负荷预测方法，前者用户可以通过个性化模型进行定制预测，后者则在保证预测性能的同时有效降低了联邦学习的通信开销，两者都在真实数据集上进行了实验验证。

图 1.1 对本文的研究方法进行了总结概括。本文的主要研究工作以及章节安排如下：

第一章 绪论。首先介绍了居民用电数据的特点和负荷预测工作的相关研究背景及意义，然后介绍了负荷预测方法当前的国内外研究现状并分析了其在隐私保护方向存在的问题。最后对本文主要的研究内容和章节安排进行了详细介绍。

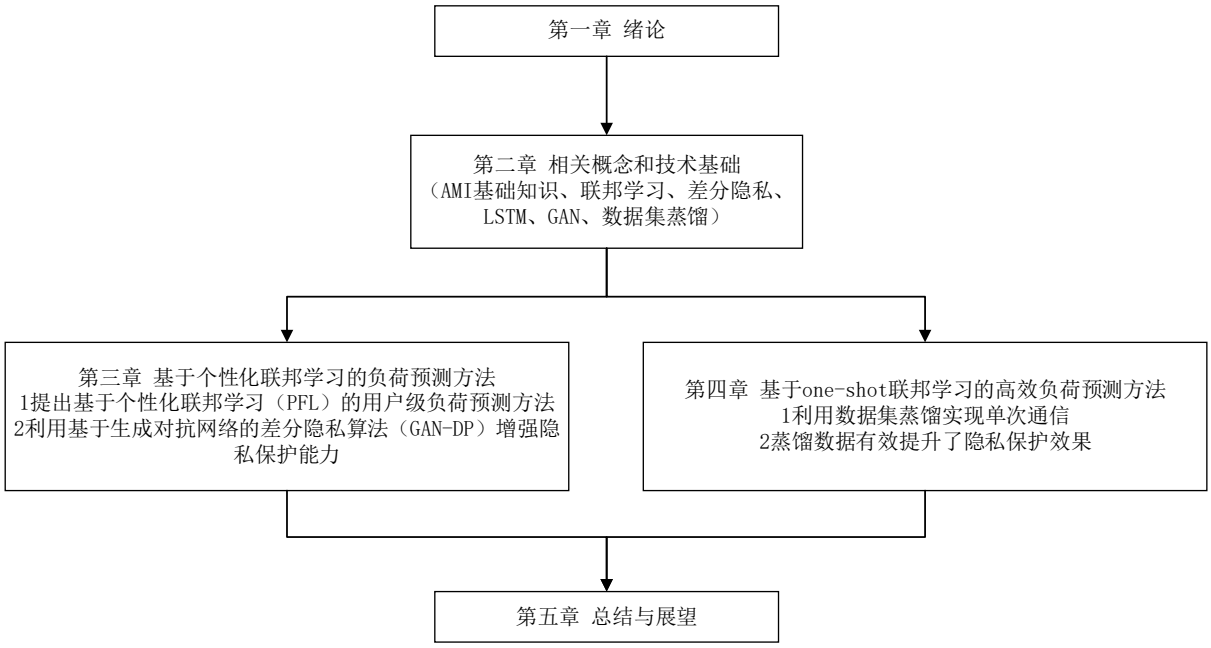


图 1.1 本文整体框架图

Fig.1.1 The overall framework of this article

第二章 相关概念和技术基础。本章内容主要介绍了本文涉及到的相关概念及基础技术知识。首先介绍了高级量测体系的工作原理及所面临的安全威胁，然后主要介绍联邦学习的基本工作原理以及它在个性化、隐私增强和高效通信方向上的研究进展，最后则是对差分隐私、长短期记忆网络、生成对抗网络和数据集蒸馏的基本工作原理进行了

中国知网 https://www.cnki.net

介绍。

第三章 基于个性化联邦学习的负荷预测方法。针对现有的基于联邦学习的负荷预测方法在数据异质性和隐私泄露前面临的挑战，本文提出了一个基于个性化联邦学习的用户级负荷预测方法，用户可以通过个性化模型进行定制预测，同时得到的全局模型可以有效预测区域用电数据，拓宽了负荷预测系统的应用场景。这里进一步应用 GAN-DP 算法来增加整体的隐私保护性能，同时最大限度地减少对预测精度的影响。实验结果表明，所提方法能够准确地预测用户级负荷并保护隐私。

第四章 基于 one-shot 联邦学习的高效负荷预测方法。为应对负荷预测场景下联邦学习的高额通信开销问题，本文从减少客户端和服务器的通信次数的角度出发，设计了一种基于单次联邦学习(one-shot FL)的高效负荷预测方法。这里使用数据集蒸馏的方法对用户原始数据集进行压缩，蒸馏数据可以学习到原始数据中最鲜明的数据特征。然后将蒸馏数据发送到服务器端进行组合，并在合成的蒸馏数据集上对全局模型进行训练。实验结果表明，所提出的预测方法通信成本要远低于传统方法，蒸馏数据也能有效的防止被窃听攻击者利用。

第五章 总结与展望：对全文的主要研究内容进行概括总结，反思研究中存在的一些问题，并对未来可能的研究方向进行了展望。

中国知网 https://www.cnki.net

中国知网 https://www.cnki.net

第二章 相关概念和技术基础

2.1 引言

本章主要对电力负荷预测领域的相关概念和涉及到的基础深度学习模型进行了介绍。首先描述了高级量测体系的工作原理和面临的安全威胁，然后针对本文所提工作中涉及到的相关技术，主要介绍联邦学习，差分隐私，长短期记忆网络和生成对抗网络的基础理论，并梳理了相关技术的发展过程及其在各领域中的应用。

2.2 AMI 基础知识

作为智能电网的重要组成部分，高级量测体系 AMI 是用来测量、收集、储存、分析和运用用电信息的支撑系统[38]。在这里，先简要介绍 AMI 框架中的数据传输过程。

图 2.1 描述了 AMI 的框架结构，具体可分为用户侧、广域网和应用侧。智能电表是用户侧的核心设备，主要负责在特定时间间隔内收集和传输客户消费数据。近年来，智能家居、智能手机、个人电脑等物联网设备作为用户侧的功能外延，可以对用户用电数据进行更多的处理运算。事实上，使用现有技术[39]智能电表直接与云通信已被证明是可行的。广域网主要负责实现用户侧和应用侧的双向通信，通信方式有光纤、蜂窝网络、卫星通信等手段。在应用侧，主要由电网计量管理服务器（Metering Data Management System，MDMS）充当 AMI 管理、存储和分析客户消费数据的控制中心。

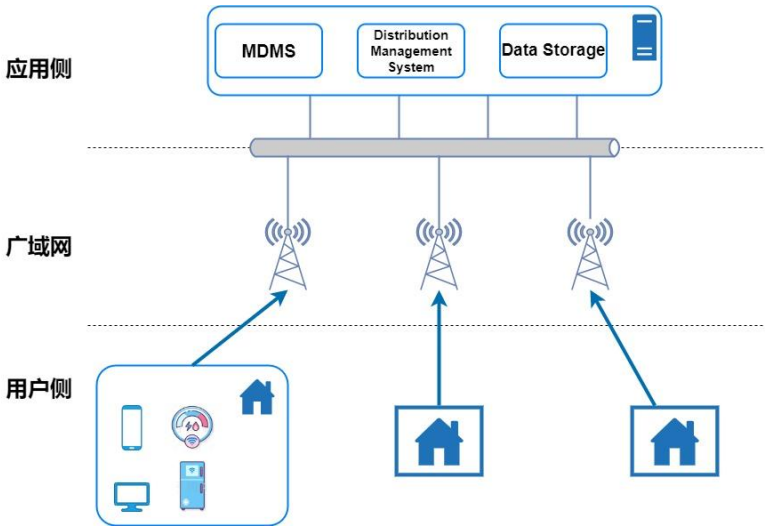


图 2.1 AMI 框架图

Fig.2.1 AMI architecture

在 AMI 的实际工作流程中，智能电表负责记录用电客户的消费情况并将这些信息传递给 AMI 应用侧。同时 AMI 还负责实现控制命令（如远程控制客户的设备和设备，以便管理负载和需求）和分发电力价格信号（如鼓励客户根据 AMI 发送的这些价格信

中国知网 https://www.cnki.net

号减少高峰负载期间的消耗）。

在逐步走向信息共享的今天，AMI 这样一个在智能电网中负责信息交互的系统一旦被恶意攻击，很有可能会对社会基础设施和用户隐私造成巨大损害，因此亟需部署安全防护措施来确保 AMI 的安全通信，提高智能电网的可靠性。AMI 面临的许多安全威胁同传统 IT 网络类似，但出于自身的构造特点，AMI 也存在一些独特的安全需求，比如用户侧储存了大量敏感隐私数据；用户侧包含大量的终端设备，并且这些设备在计算能力、存储能力和安全保护能力上都有不足；对 AMI 的严重攻击会波及到智能电网的正常运作等等。

当前 AMI 面临的安全威胁主要是机密性、完整性、可用性和不可否认性[40]。机密性要求用电数据仅可被授权实体进行访问，并且在电力信息通信时不能发生有意或无意的数据泄露情况。当 AMI 检测到用电数据等原始内容泄露时，需要采取相应的安全措施来防止恶意攻击者进一步窃取用户隐私信息。完整性是指传输的数据必须真实完整，能够真实反映源头数据的意图，没有未经授权进行的修改、删除或添加操作。这里的数据不单指用户的原始用电数据和用电信息，也包含 AMI 下发的控制指令，恶意修改的非法控制指令也可能会对整个电网系统造成严重破坏。可用性要求授权实体可以在需要时对数据信息进行访问，这就对 AMI 的用户侧、广域网、应用侧的每个环节都提出了安全要求，这样才能保证信息通信（尤其是控制指令）可以准确无误的进行。不可否认性表现为问责制，即要求接收数据的实体和发送数据的实体承认自己的操作，不允许欺骗行为发生。交互的审计日志是确保问责性的常用方法，可以有效防止实际工作中因无法验证错误决策而出现的互相推卸责任的情况。

2.3 联邦学习

2.3.1 联邦学习基本原理

联邦学习[41]是一种新兴的机器学习算法框架，最初由谷歌于 2016 年提出，用来解决安卓手机终端用户在本地对语言预测模型进行更新的问题。联邦学习的设计目标是在合法合规的前提下保障大数据交换过程中的隐私和数据安全，因此它被设计为不需要直接数据交换或者收集数据的形式，在保护用户隐私的同时也解决了人工智能产业面临的数据孤岛困境。

联邦学习实质上是一个分布式机器学习框架，旨在建立一个基于分布数据集的联邦学习模型。在联邦学习框架下，要有不少于两个客户端节点将在中央服务器的协作下共同训练一个全局模型，且在全局模型训练过程中要求原始数据不出本地。联邦学习工作原理如图 2.2 所示。共享的全局模型由参与设备组成的联邦进行训练，该联邦由中央服

中国知网 https://www.cnki.net

务器主持。这种方法使边缘节点能够协同地在本地训练模型，而无需共享原始训练数据。这里本地模型参数更新（如梯度）会代替训练数据被上传到中央服务器用来更新全局模型，中央服务器会聚合这些参数更新并生成新一轮的全局模型，如此循环往复直至全局模型收敛。当以加权平均的方式计算这种聚合时，这种联合训练的方法被称为联邦平均算法[30]（Federated Average，FedAvg），是当前联邦学习研究领域的常用基准模型。

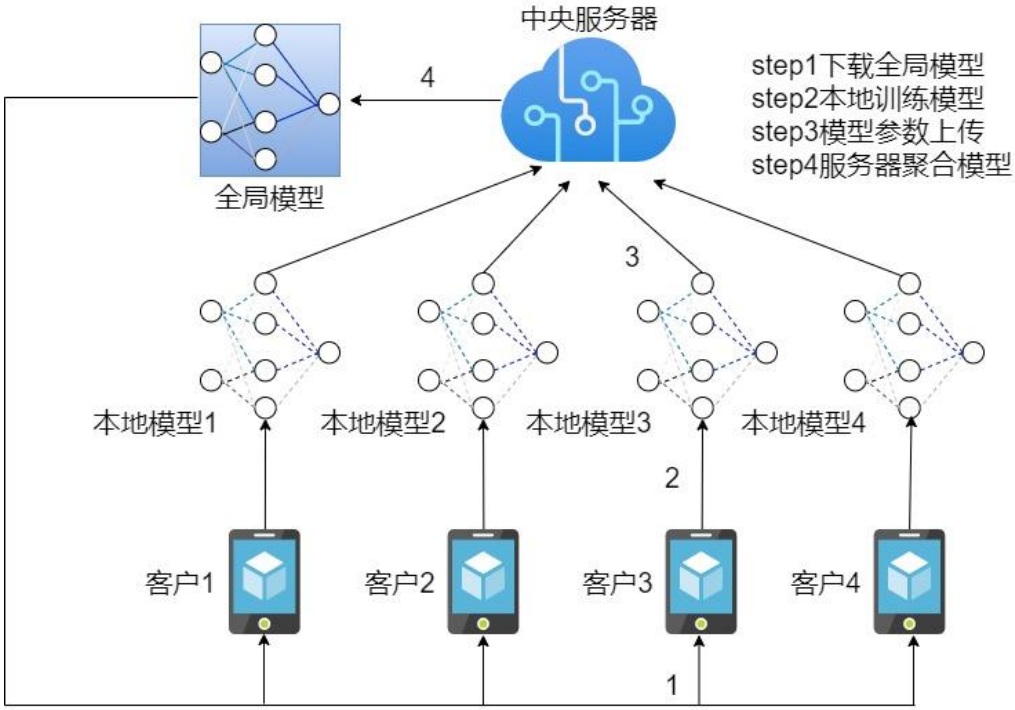


图 2.2 联邦学习工作原理

Fig.2.2 The operating principle of FL

2.3.2 隐私增强联邦学习

标准 FL 的中心服务器是一个易攻击处，因此基于区块链的去中心化 FL[42]是防御单点故障，缓解对中心服务器过度依赖的有效方法。此外，还有一些常用的隐私保护技术，如安全多方计算[43]、同态加密[44]和差分隐私[45]。安全多方计算是一种基于密码学的隐私计算算法协议，可以看作是多种密码学基础工具的综合应用。同态加密是一种不需要对密文进行解密的密文计算解决方案，它允许对密文进行加法和乘法运算。这两者虽然可以实现较高的隐密性和准确的计算结果，但对计算和通信能力的要求也比较高。差分隐私定义了一种严格的隐私保护模型，它通过在待处理数据集中添加服从一定分布的随机噪声，得到新的受干扰数据集，以此来对数据隐私进行保护。然而，添加噪声导致的数据效用降低问题需要解决。

2.3.3 个性化联邦学习

使用 FL 来训练神经网络通常会遇到非独立同分布(not independent and identically

中国知网 https://www.cnki.net

distributed, non-IID)数据[46]的问题。传统 FL 通过聚合这些不同的模型更新创建全局模型，但该模型只能获得参与训练客户的共同特征，所以在特定用户数据上可能表现不佳。为了解决这些问题，人们提出个性化联邦学习（Personalized Federated Learning，PFL）为联邦中的每个客户提供个性化的模型。Li 等人[47]提出了 FedMD 方法，它使客户能够使用基于迁移学习的本地数据来训练独立模型。每个客户端首先在公共数据集上训练模型来执行迁移学习，然后在 FL 训练阶段之前基于本地数据对模型进行微调。Wang 等人[48]提出了 FAVOR 框架，该框架会在联邦学习的每个迭代轮次选择一部分参与训练的客户端，这样可以有效减少 non-IID 数据带来的偏差，提升模型表现。Arivazhagan 等人[49]为深度神经网络设计了一个基础层+个性化层的结构。基础层与中心服务器共享数据，个性化层则在客户端保持私有性，用于本地训练。

2.3.4 高效通信联邦学习

联邦学习模型训练依赖于客户端和服务器间频繁的数据交换，这种交互模式更新所造成的高昂的通信开销阻碍了它的发展和广泛应用，因此，尽可能降低联邦学习的通信开销变得至关重要。目前，降低联邦学习通信开销的方法[50]主要集中在减少客户端和服务器之间的通信次数和减少每次通信中传输的数据量这两种方法上。

为了减少客户端和服务器之间的通信次数，Guha 等人[50]提出了一种单轮通信联邦学习方案，在标准联邦学习框架上要求其中所有训练都在客户端本地执行，在训练结束时仅通过一次通信将各客户端的本地模型发送至服务器端进行聚合。Yao 等人[52]第一个采用双流模型在联邦学习设置上训练，并在训练迭代中引入最大均值差（MMD）约束。通过最小化 MMD 损失，使得双流模型可以提取更多的广义特征，在不影响最终性能的表现下加速模型收敛，达到减少客户端和服务器之间通信次数的目的。除此之外，一些研究采用选择性通信策略来减少客户端和服务器之间的通信次数。Luping 等人[53]提出在每个客户端完成本地训练即将上传更新前，对本地模型的更新趋势同全局模型的更新趋势进行比较选择，选择上传同全局模型优化趋势相似的客户端模型参数更新，以此提高全局模型收敛速度。Tao 等人[54]则是对梯度进行选择，他们提出的边际随机梯度下降算法，要求每次上传更新时中只选择重要的梯度上传至服务器。不同于上述两种方法，考虑到移动边缘计算结构下边缘服务器的传播时延要小于客户端和服务器通信，Liu 等人[55]在联邦学习框架的客户端和中央服务器之间引入边缘服务器作为中间参数聚合器，有效减少了通信开销。

减小每次通信传输的数据规模可以通过机器学习压缩技术来实现。Konečný 等人[56]就提出了轮廓更新和结构更新两种模型参数更新策略。此外，考虑到在联邦学习中模型

中国知网 https://www.cnki.net

结构共享，因此可以通过对模型参数进行压缩来降低通信成本，比如网络剪枝、量化和权值共享等方案[57]。对于特定的网络模型可以有特定的压缩方法，比如 Huang 等人[58]提出了一种专门用于压缩卷积神经网络结构的模型。与压缩模型参数类似，如果客户端在联邦学习过程中上传的模型更新参数是梯度信息，则可以对梯度进行压缩，如 Shokri 等人[59]提出的深度梯度压缩方案、Alistarh 等人[60]提出的梯度量化和编码。上述这些方法虽然经由数据压缩降低了传输的数据规模，但由于噪声的引入使得压缩算法不能收敛到接近最优解，进而降低了算法性能表现[61]。

2.4 差分隐私

差分隐私（Differential Privacy，DP）是 2006 年 Dwork 首次提出的一种严格可证明的隐私定义[62]，其基本思想是当敌人试图从数据库中查询个体信息时将其混淆，使得敌手无法从查询结果中辨别到个体级别的敏感性。假设这样一个机器学习场景，其中机器学习算法随机设置，可以通过在学习目标模型时在数据中加入噪声来满足差分隐私机制，实现隐私保护的目的。相关定义如下所示：

敏感度：假定两个只有一个样本数据不同的数据集D，D'，对于任意域的函数$f: D \to R^d$的敏感度是

$$\Delta f = \max_{D,D'} \|f(D) - f(D')\|_p \tag{2.1}$$

其中$\|\cdot\|_p$表示 L_p范数。敏感度用来量化由于添加或删除单个样本影响差分隐私机制输出的最大程度。

$(\varepsilon, 0)$差分隐私：设 M: $D^n \to R^d$是一个随机函数，$\varepsilon > 0$。如果对只有一个数据记录不同的两个数据集D, D'和任意可能的输出集合S，M满足

$$\Pr\{\mathrm{M}(D) \in S\} \leq e^{\varepsilon} \Pr\{\mathrm{M}(D') \in S\} \tag{2.2}$$

则称M满足$(\varepsilon, 0)$差分隐私。其中ε被称为隐私预算，它的值越小，说明隐私保护效果越好，但相应的需要引入更多的噪声，最终导致较多的精度损失。因此，如何权衡数据的实用性和隐私性是差分隐私的重要研究方向。

(ε, δ)差分隐私：设M: $D^n \to R^d$是一个随机函数，$\varepsilon, \delta > 0$。如果对只有一个数据记录不同的两个数据集D, D'和任意可能的输出集合S，M满足

$$\Pr\{\mathrm{M}(D) \in S\} \leq e^{\varepsilon} \Pr\{\mathrm{M}(D') \in S\} + \delta \tag{2.3}$$

则称M满足(ε, δ)差分隐私。

为了满足差分隐私的约束条件，在对数据进行处理操作时不同的数据往往会采用相应的操作机制[63]。在差分隐私领域中，处理数值型数据时常采用拉普拉斯机制和高斯机

中国知网 https://www.cnki.net

制。其中，拉普拉斯机制使用服从拉普拉斯分布的数据噪声扰动数据，该机制满足$(\varepsilon,0)$差分隐私；而高斯机制则使用服从高斯分布的数据噪声对数据进行扰动，其机制满足(ε,δ)差分隐私。

2.5 LSTM 介绍

随着递归次数增多，RNN 网络在损失反向传播时会出现梯度的不稳定场景，比如梯度爆炸和梯度消失，梯度爆炸会使网络无法收敛，而梯度消失则会导致网络无法更新参数，两者都会使网络无法通过训练提取序列的上下文信息。为了解决这一问题，长短期记忆网络（Long-Short Term Memory，LSTM）由 Hochreiter 等人于 1997 年首次提出，通过对标准 RNN 网络中的隐藏层进行改进，LSTM 可以更加简单高效的记忆长期信息，解决了标准 RNN 面临的长期依赖问题（即梯度消失和梯度爆炸），而且 LSTM 在时间序列数据的分析处理上要明显优于其它现有的神经网络模型。

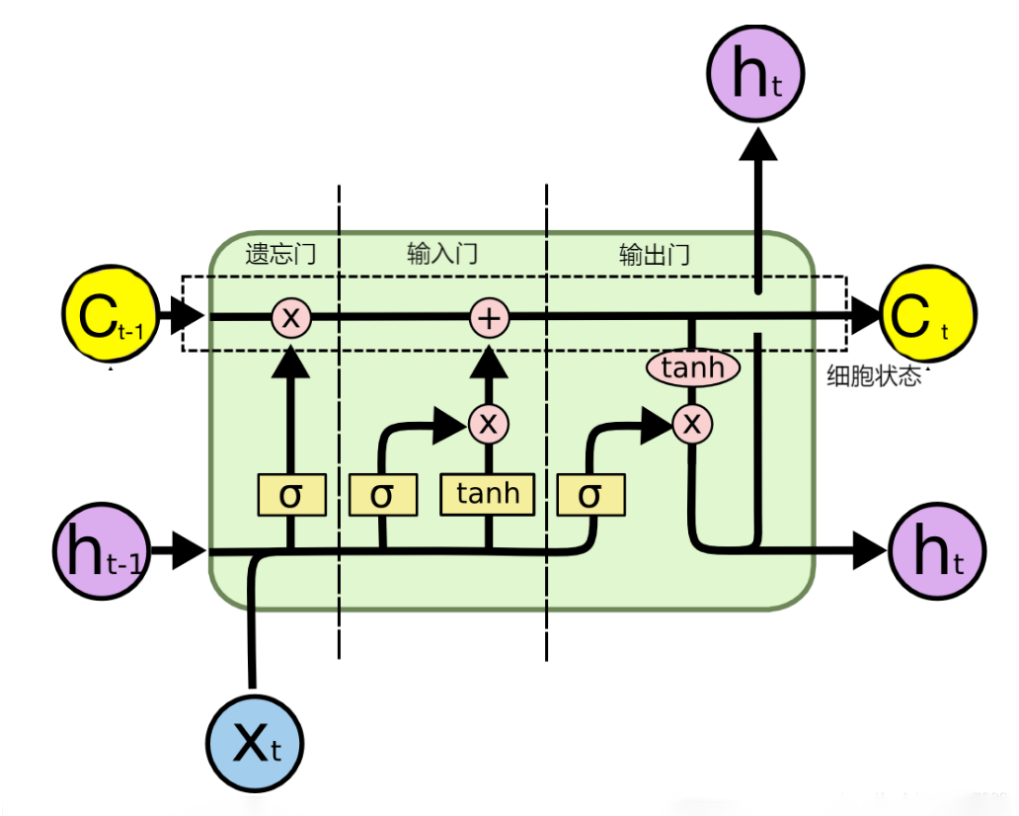


图 2.3 LSTM 的网络结构

Fig.2.3 The structure of LSTM

LSTM 的网络结构如图 2.3 所示。细胞状态（cell state）是 LSTM 网络中的一大核心部件，在图 2.3 中表现为上方水平的那一条贯穿整个循环核的数据流向线，其功能为保证信息在模型传递的过程中不会丢失。LSTM 模型的另外一个核心就是控制细胞状态中的信息/数据被移除或增加的结构，这个结构叫做门（gates）。LSTM 就是依靠网络中

中国知网 https://www.cnki.net

的遗忘门、输入门及输出门对有益的信息加以传播，对无效的内容进行遗忘，进而来实现其长期记忆功能。

具体来说，LSTM 利用遗忘门来表示上一时刻单元状态C_{t-1}中信息需要忘记什么,其公式下所示：

$$f_t = \sigma(W[h_{t-1}, x_t] + b) \tag{2.4}$$

其中σ是 sigmoid 激活函数，W为权重矩阵，b为偏置值，h_{t-1}，x_t分别表示为上一时刻的输出值和当前时刻的输入值。

然后输入门用来确定当前时刻的输入x_t有多少需要保存在当前时刻单元状态C_t中，此时输入门的 sigmoid 层用来确定信息更新内容, tanh 层则生成新增候选值向量添加至当前状态。相应公式如式（2.5）、（2.6）所示：

$$i_t = \sigma(W[h_{t-1}, x_t] + b) \tag{2.5}$$

$$\tilde{C}_t = \tanh(W[h_{t-1}, x_t] + b) \tag{2.6}$$

按照 LSTM 的网络结构，当前时刻的单元状态C_t也随之进行状态更新，其公式下所示：

$$C_t = f_t * C_{t-1} + i_t * \widetilde{C_t} \tag{2.7}$$

其中$*$指两向量中元素按位相乘。

最后，LSTM 还可根据输出门确定该单元状态C_t有多少需要传递到下一单元中。其公式如式（2.8）、（2.9）所示：

$$O_t = \sigma(W[h_{t-1}, x_t] + b) \tag{2.8}$$

$$h_t = O_t * \tanh(C_t) \tag{2.9}$$

2.6 GAN 介绍

生成对抗网络（Generative Adversarial Network，GAN）是 Ian J.Goodfellow 等人[64]在2014年提出的一种无监督生成模型,博弈论中的纳什平衡是该模型的核心数学思想。GAN 的提出突破了以往生成模型存在的问题，提高了模型的泛化能力。GAN 作为一种功能强大的深度学习方法，已广泛应用于图像学习、数据处理、文本挖掘等[65]各个非结构化数据领域。

GAN 的基本结构如图 2.4 所示，可以看出 GAN 主要由生成器（Generator，G）和鉴别器（Discriminator，D）两部分组成，其基本思想是生成器通过学习真实数据样本，

中国知网 https://www.cnki.net

尽可能逼真地生成假数据样本，鉴别器用于判断生成的样本与真实样本是否不同。在训练过程中两个模型不断对抗、迭代优化，生成器最终能够生成了一组鉴别器也无法区分真伪的“假样本”，这样生成器和鉴别器便达到一个稳态，这就是纳什均衡点，此时整个网络收敛。鉴别器对生成样本的误判上表明生成样本与真实样本表现出了相似的数据特征。

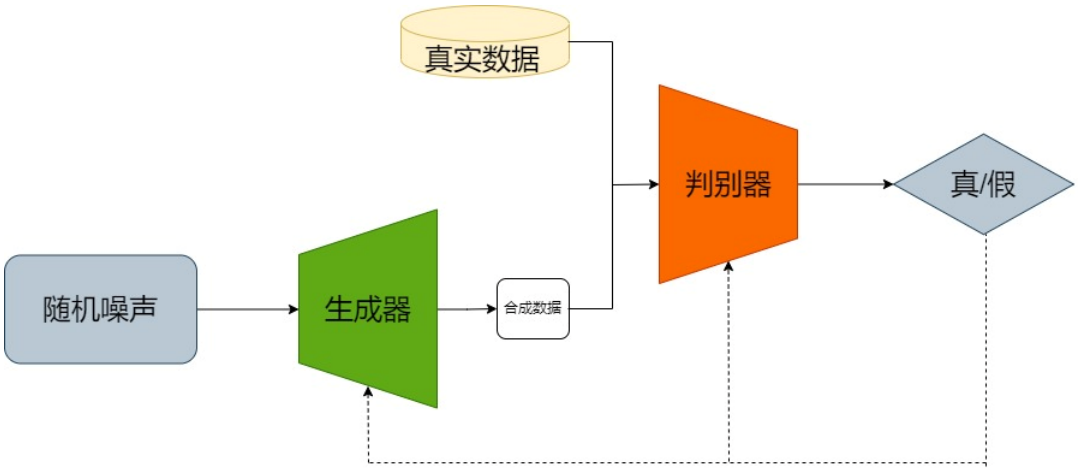


图 2.4 GAN 的结构图

Fig.2.4 The structure of GAN

生成器和鉴别器的博弈关系是关于函数$V(G,D)$的极小极大化问题，在博弈过程中，D 的任务是最大化的识别真实数据和生成数据，G 的任务是最小化生成的数据与真实样本的分布，这两个优化过程同时进行且互相博弈，这个动态博弈的过程如式（2.10）所示：

$$\min_G \max_D V(G,D) = E_{X\sim p_{\text{data}(x)}}[\log D(x)] + E_{z\sim p_z(z)}\left[\log\left(1-D\left(G(z)\right)\right)\right] \tag{2.10}$$

其中，随机输入噪声z分布为$p_z(z)$，真实数据x分布为$p_{\text{data}(x)}$，$G(z)$为随机噪声经过生成器生成的数据，$D(x)$输出 0 到 1 之间的任意值，表示鉴别器判断x是否为真的概率，$D(G(z))$则代表鉴别器判断生成数据$G(z)$是否为真的概率。

2.7 数据集蒸馏

蒸馏技术本质上就是对原始信息进行压缩处理，不同的是数据集蒸馏压缩的对象是数据集，而知识蒸馏的压缩对象则是模型。知识蒸馏通过定义教师网络（大型神经网络）和学生网络（小型神经网络），在教师网络对学生网络进行诱导训练中完成知识的迁移和模型规模上的压缩。知识蒸馏技术在迁移学习的应用较为成熟，极大减轻了训练及使用重型网络模型的计算负担。知识蒸馏同联邦学习的联系也比较紧密，Jeong 等人[66]提出了基于知识蒸馏的联邦学习算法，在减轻 non-IID 问题对模型负面影响的同时也有效

中国知网 https://www.cnki.net

降低了联邦训练的通信开销。Jiang 等人[67]提出了一种个性化联邦学习算法，通过知识蒸馏技术将全局模型的知识迁移至小模型上，并在各客户端的本地数据上进行微调，这样每个客户端都有自己的个性化模型，有效提高了本地模型性能表现。Sattler 等人[68]对现有的联邦蒸馏方法进行改进，提出一种更为高效通信的压缩联合蒸馏算法，在固定性能目标的前提，同基准模型相比大大减少了所需的通信开销。

数据集蒸馏的目的则是将原有的大规模数据集压缩合成为信息损失小的小数据集，以降低存储和训练成本。Wang 等人[69]第一个正式提出数据集蒸馏这个方法，该方法将常规优化器建模为将合成数据集作为输入的函数，并使用额外的优化器逐像素地对合成图像数据集进行更新。Sucholutsky 等人[70]提出了“软”标签的概念，为每个合成样本分配一个由提取图像和标签组成的标签分布，该研究将数据集蒸馏方法的对象从图像数据扩展到文本数据，并都取得了不错的性能表现。后续对数据集蒸馏的改进主要基于优化的方法，通过合成受各种优化目标约束的图像样本来实现蒸馏。Zhao 等人[71]提出了一种用于数据高效学习的训练集合成技术，它将数据集蒸馏问题定义为在原始数据和合成数据上训练的深度神经网络间的梯度匹配问题。Cazenavette 等人[72]提出利用训练轨迹匹配的方式，通过在合成数据上训练的参数轨迹段与在真实数据上训练模型中预先记录的轨迹段相匹配，让蒸馏数据实现同真实数据相近的测试性能。数据集蒸馏可以加快模型训练，降低通信成本，因此它在持续学习[73]、神经架构搜索[74]、隐私保护任务[75]等机器学习任务中都发挥着重要作用。

2.8 本章小结

本章内容主要介绍了本文涉及到的相关概念及基础技术知识。在 2.2 中介绍了 AMI 体系的工作原理及所面临的安全威胁，2.3 主要介绍联邦学习的基本工作原理以及它在个性化、隐私增强和高效通信方向上的研究进展，余下 4 节则是分别对差分隐私、长短期记忆网络、生成对抗网络和数据集蒸馏的基本工作原理进行了介绍。

中国知网 https://www.cnki.net

中国知网 https://www.cnki.net

第三章 基于个性化联邦学习的负荷预测方法

3.1 引言

准确的负荷预测对于电力生产、传输和维护至关重要。当前深度学习模型已经取代其他经典模型成为最流行的预测模型。但深度预测模型需要用户提供大量的私人用电量数据，这一行为存在潜在的隐私泄露风险。作为一种新型的分布式机器学习技术，联邦学习只发送模型参数更新，不共享原始数据，通过聚合更新对全局模型进行联邦训练。然而，现有的基于联邦学习的负荷预测方法仍然面临着数据异质性和隐私泄露的挑战。

基于上面讨论的情况，本文的主要贡献如下所示：

（1）提出了一种基于个性化联邦学习（PFL）的用户级负荷预测方法，该方法可以获得每个客户端的个性化模型和全局模型。个性化模型在使用本地用电负荷数据进行预测时表现要优于全局模型，而全局模型在区域电力负荷预测上也能发挥积极作用。

（2）利用一种基于生成对抗网络的差分隐私算法（GAN-DP）来增强该方法的隐私保护能力。该算法在本地模型参数中加入可调噪声以满足差分隐私要求，并基于 GAN 理论实现了隐私保护和预测精度之间的平衡。

（3）在真实数据集上进行了大量的实验。本文评估了个性化模型的实验性能和负荷预测系统的隐私保护能力。最终结果表明，该方法性能要优于基准模型，初步展示了应用前景。

3.2 预测模型说明

3.2.1 模型总览

图 3.1 描述了本工作的整个系统架构。从图中可以清楚地看出，整个系统主要由两个部分组成：中央服务器和客户端。在负荷预测场景中，电力公司是中央服务器的主体，依靠智能电网进行电力传输和管理。用电住户在这里被定义为客户端，他们可以测量电力消耗，训练本地模型，并与中央服务器通信。这里将该系统的具体步骤总结如下。

全局模型初始化：在正式开始训练前，每个客户端会接收来自中央服务器的初始全局权重值。该初始权重值通过分配随机值来初始化。

本地模型训练：在使用从服务器下载的权重值来更新本地参数后，各客户端使用本地私有数据来训练本地模型。

本地模型参数合成：在 GAN-DP 中，生成器接收经过训练的本地模型参数，输出一组合成参数。然后合成数据会注入鉴别器和 DPI，以查看它是否满足两者的要求。一旦满足要求，该合成数据就被当作本地模型参数来参与后续步骤。

中国知网 https://www.cnki.net

个性化模型更新：这里按照 Ditto 设置来更新每个客户端的个性化模型参数。

本地模型参数上传：每个参与训练的客户端将合成参数上传到中央服务器。

全局聚合：通过聚合上传到中央服务器的模型更新生成新的全局模型参数。

全局模型更新：全局模型使用聚合生成的参数执行权重更新。

模型广播：更新后的权重由中央服务器广播回客户端，用于下一轮训练。

上述迭代将继续进行，直到各自的模型（包括全局模型和个性化模型）收敛为止。

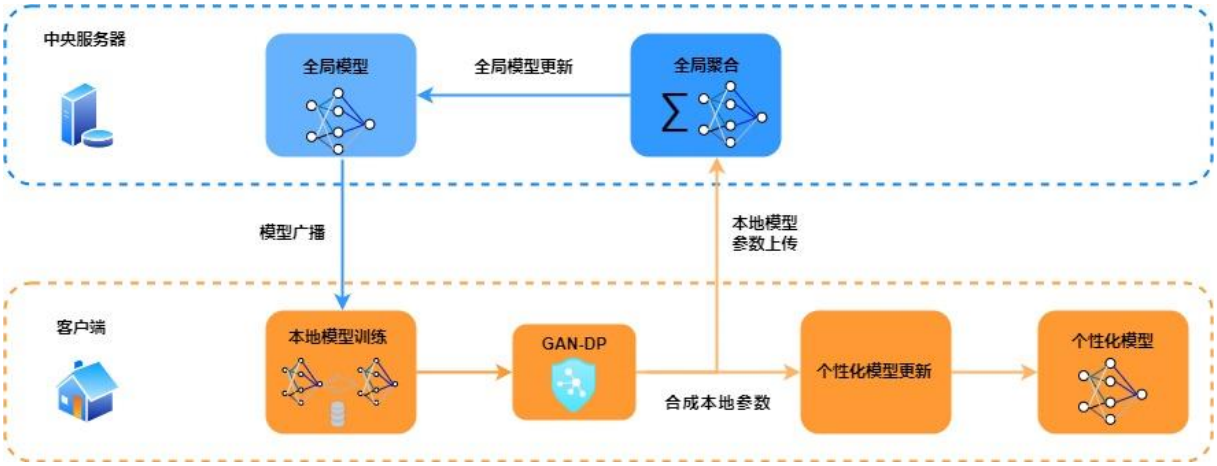


图 3.1 系统架构

Fig.3.1 System architecture.

3.2.2 个性化联邦学习模型

传统 FL 允许多个客户机协同训练一个全局模型。总的来说，全局目标是要解决：

$$\min_{\omega} f(\omega) = \sum_{k=1}^{N} p_k F_k(\omega) \tag{3.1}$$

其中N是设备的数量，$F_k(\omega)$为设备k的本地目标，在 FedAvg 设置中，p_k为非负权重值，这里可以设置$p_k = \frac{n_k}{n}$，$\sum_{k=1}^{N} p_k = 1$，其中，每个设备k上有n_k个样本，$n = \sum_{k=1}^{N} n_k$为总数据样本数。

但事实上，不同设备上的本地数据x_k呈现不同的数据分布$\mathcal{D}_k$，即$F_k(\omega) = \mathbb{E}_{x_k \sim \mathcal{D}_k}[f_k(\omega; x_k)]$，而且 FL 训练的全局模型在特定客户数据上的预测表现较差。为解决数据异构问题，有必要对于每个客户分别建立个性化的模型$\{v_k\}_{k\in[N]}$。这里使用 Ditto[76] 这样一个多任务 FL 框架来定制个性化模型。与其他个性化策略相比，Ditto 体积更小，效率更高，更重要的是，Ditto 更适合现实场景设置，因为它可以同时考虑到几个约束（准确性、公平性和稳健性）的相互影响。而且由于其多任务学习的结构设计，该方法还可以同时获得全局模型和每个客户的个性化模型。个性化模型在特定用户用电数据的预测精度上优于全局模型。尽管全局模型在单个用户的预测表现不佳，但全局模型可以用于预测区域负荷（详见 3.4 节），这极大拓宽了该方法的应用面。全局目标与本地个

中国知网 https://www.cnki.net

性化目标之间的双层优化问题可表示为：

$$\min_{v_k} h_k(v_k;\omega^*) \coloneqq F_k(v_k) + \frac{\lambda}{2}\|v_k - \omega^*\|^2, \quad \text{s.t. } \omega^* \in \arg\min_{\omega} f(\omega) \tag{3.2}$$

其中超参数λ是用来调整全局和本地模型之间的插值。特别地，当$\lambda \to +\infty$时 Ditto 的结果近似于全局模型，当$\lambda \to 0$时 Ditto 将更接近于训练本地模型。

如上所述，这里通过 Ditto 联合训练全局模型ω^*和本地个性化模型$\{v_k\}_{k\in[N]}$。对于客户端$k \in S_t$（S_t指本次迭代中参与训练的设备数量），每个参与训练的客户端将利用其本地数据在第t次迭代时训练各自的本地模型：

$$\omega_k^{t+1} \leftarrow \omega^t - \eta_g \nabla F_k(\omega_k^t) \tag{3.3}$$

在参数更新部分，这里采用全局正则化的方法并行更新个性化模型参数v_k^{t+1}：

$$v_k^{t+1} = v_k^t - \eta_l\left(\nabla F_k(v_k^t) + \lambda(v_k^t - \omega^t)\right) \tag{3.4}$$

其中η_g和η_l分别对应更新全局模型和个性化模型时的不同学习率。在同一阶段，在这里使用 FedAvg（或其他优化策略）对全局模型参数ω^{t+1}进行更新：

$$\omega^{t+1} \leftarrow \omega^t + \frac{1}{|S_t|}\sum_{k\in S_t}(\omega_k^{t+1} - \omega_k^t) \tag{3.5}$$

这个迭代过程将不断重复，直到模型收敛或达到训练轮次的预设值，最后得到全局模型ω^*和每个客户各自的本地个性化模型$\{v_k\}_{k\in[N]}$。

3.2.3 面向 PFL 的 GAN-DP 建模

在联邦学习中使用差分隐私算法是使整体框架获得强大隐私保障的有效途径。然而，差分隐私在精度上的牺牲阻碍了其进入实际应用场景。在上述 FL 设置下，这里引入一种基于 GAN 的 DP 算法 GAN-DP[77]，使所提方法在满足差分隐私要求的同时提高了负荷预测精度。

如图 3.2 所示，GAN-DP 包含生成器、鉴别器和结构类似于鉴别器的 DP 标识符(DPI)。在本文系统中，本地参数是由客户端通过本地训练获得的。之后将本地模型参数输入生成器，此时生成器会生成一组合成参数。这里将生成的合成参数输入鉴别器和 DPI，如果合成参数能同时满足这两个感知器的要求，则将该参数作为输出结果，进入后续操作。表 3.1 提供了本节符号的简要说明。

中国知网 https://www.cnki.net

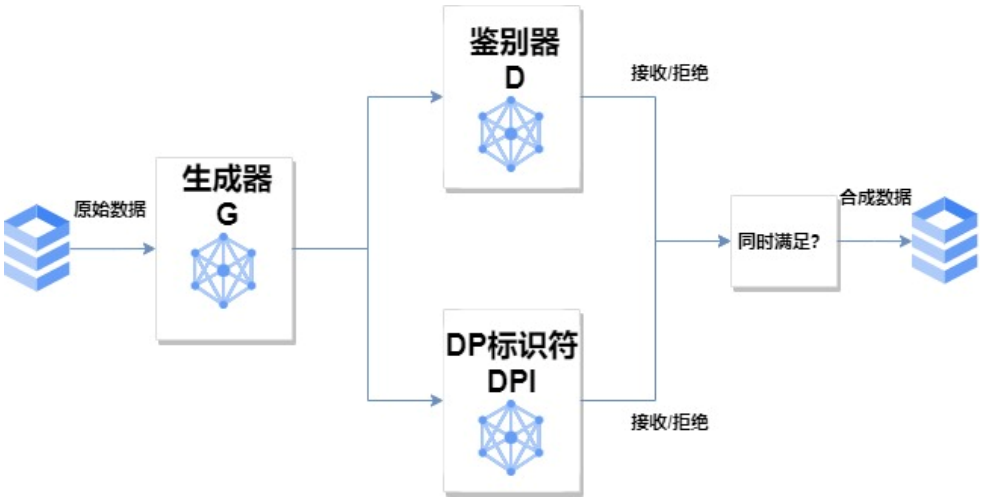


图 3.2 GAN-DP 结构图
Fig. 3.2 The framework of GAN

表 3.1 GAN-DP 中的参数说明
Tab.3.1 Notations in GAN-DP

符号	解释
d_i	训练数据
N_{d_i}	噪声样本数量
p_g	噪声样本数据分布
$\delta(d_i)$	训练数据样本
$E(\cdot)$	数学期望
$p_g(y)$	预先注入的噪声样本
$G(y;\theta_g)$	生成器结构
$D(y;\theta_d)$	鉴别器结构
$I(y;\theta_i)$	DP 标识符结构
$S(D;I)$	交互式鉴别器和标识符所组成的新结构

生成器：生成器利用原始的本地模型参数来生成合成参数，并将其提交给鉴别器进行识别。数量为N_{d_i}的噪声样本$\{y_1, y_2, \dots, y_n\}$（服从$p_g(y)$）会经由下述方式进行更新：

$$\nabla_{\theta_g} \frac{1}{N_{d_i}} \sum_{i=1}^{N_{d_i}} \log\left(1 - D\left(G(y_i)\right)\right) \tag{3.6}$$

鉴别器：经过多次迭代，如果鉴别器将合成参数识别为原始模型参数，则将其视为最终结果。这里从$\delta(d_i)$选取数量为N_{d_i}的数据样本$\left\{d_1, d_2, \dots, d_{N_{d_i}}\right\}$，鉴别器在更新过程中的梯度上升可表示为：

$$\nabla_{\theta_d} \frac{1}{N_{d_i}} \sum_{i=1}^{N_{d_i}} \left[\log D(d_i) + \log\left(1 - D\left(G(y_i)\right)\right)\right] \tag{3.7}$$

DP 标识符：由于 DPI 的功能同鉴别器类似，这里鉴别器和 DPI 与生成器并行地进行交互。与鉴别器不同，DPI 试图确认合成的模型参数是否满足 DP 要求。这里的更新

中国知网 https://www.cnki.net

过程可以表示为：

$$\nabla_{\theta_{N_{d_i}}} \frac{1}{N_{d_i}} \sum_{i=1}^{N_{d_i}} \times \left[\log S(d_i \mid D; I) + \log\left(1 - S(G(y_i) \mid D; I)\right)\right] \tag{3.8}$$

在 GAN-DP 中，生成器、鉴别器和 DPI 之间形成了一个最小-最大博弈问题。根据上述公式，这个问题可以被建模为：

$$\min_G \max_S E_{x\sim\delta(d_i)}[\log S(d_i \mid D; I)] + E_{y\sim p_g(y)}\left[\log\left(1 - S(G(y_i) \mid D; I)\right)\right] \tag{3.9}$$

其中用$\min_G$来降低被识别的可能性，用$\max_S$来增加欺骗的可能性。

最终，基于 PFL 的居民住宅负荷预测算法伪代码如算法 1 所示。

算法 1：基于 PFL 的居民住宅负荷预测

```
1：参数初始化
2：for 每一全局模型更新轮次 do
3：    服务器在N台设备中随机选取其中一个子集 S_t
4：    服务器向所有选中设备发送ω^t
5：    for 每一参与方并行地 do
6：        本地模型训练（公式 3.3）
7：        生成合成本地模型参数（公式 3.9）
8：        个性化模型更新（公式 3.4）
9：        发送全局参数更新（公式 3.5）
10：   end
11：   全局聚合
12：end
13：return 各客户的个性化模型；全局模型
```

3.3 数据集介绍

3.3.1 基本内容

实验中使用的数据集是“HUE[78]:不列颠哥伦比亚省建筑物每小时能源使用”数据集，目前该数据集中包括了哥伦比亚省 22 个家庭近三年的每小时能源使用数据、房屋特征数据和天气数据。其中能源使用数据以小时为单位进行采样，这样一天可以采样 24 次，每天就会有 24 个采样值，每小时能源使用数据是以千瓦时为单位记录的；房屋特征数据包括各种建筑信息，例如房屋特征类型（老式单层住宅、现代高层公寓等）、房屋朝向、周边房租情况（判断消费水平）和暖通空调类型（燃气壁炉、电暖气、固定空调等）；天气数据则采集至离住宅最近的气象站数据，包括每小时的室外温度、室外相当湿度和对当天天气的简要文字描述（如多云、晴天等）。HUE 数据集提供了来自多个家庭的长期电力消费数据，对研究部署在微电网和离网社区上的系统进行模拟和测试提供了很大帮助。下面的图 3.3 为某一居民的用电负荷数据的可视化展示图。

中国知网 https://www.cnki.net

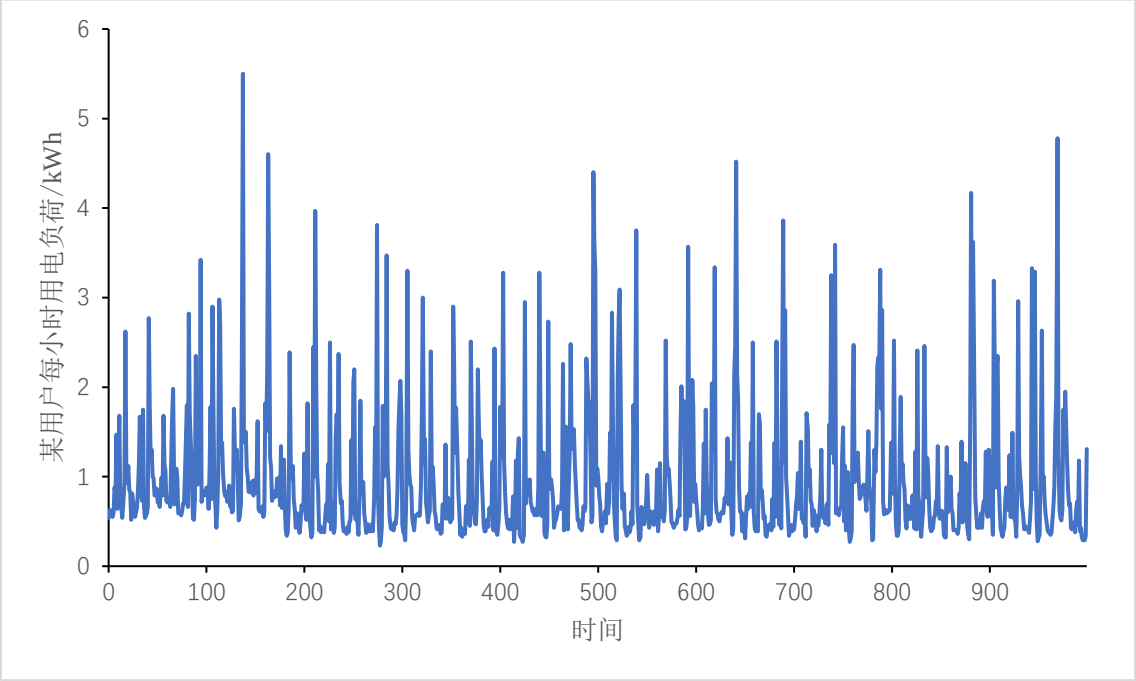


图 3.3 用电负荷数据可视化展示图

Fig.3.3 Data visualization diagram of electric load

最后需要说明的是，因为本文涉及的研究方向是联邦学习在负荷预测场景下的应用，所以后续实验中在进行负荷预测任务时只简单考虑用电负荷与时间的相关性。未来有机会会根据多属性因素对用电负荷的影响来建立更为精细的负荷预测模型。

3.3.2 居民用电负荷特性分析

掌握电力负荷的特性，准确把握电力负荷变化的基本规律和发展趋势是有效进行电力负荷预测的基本条件，对提高预测精度和预测结果的可解释性具有重要意义。使用时间序列法进行负荷预测时往往将电力负荷序列分为周期分量、非周期分量、随机变化分量和季节变化分量，可见电力负荷的变化同时具有周期性和随机性特征。

受社会生产和居民生活中各方面因素影响，诸如工厂生产任务、居民生活习惯、天气因素等都会造成电力负荷的随机化波动。电力负荷曲线也具有周期性特征，而且不同的用电主体往往会反映不同的用电周期特性[79]。大多数用电家庭表现出的是日周期特性，即以一天二十四小时为周期时用电负荷数据所体现出来的变化规律。在这一天二十四小时的区间里，不同时间段表现出不同的用电水平，比如白天的用电量要低于晚上的用电量，夜间十二点到清晨八点之间存在一段明显的用电低谷期，到了第二天又会呈现相似的变化特征。公司、工厂等用电单位反映的则是周周期特性，用电负荷数据以一周七天为周期进行规律变化。在一周当中，工作日和非工作日的用电特征差异较为明显，周一到周五之间的电力负荷曲线表现出相似变化，周六和周日也具有相似性，且在工作日的用电负荷要明显高于非工作日。这种周周期特性也比较符合实际情况，在工作日，公司、

中国知网 https://www.cnki.net

工厂整体处于社会生产阶段，需要大量的用电来满足生产需求，用电负荷处于峰值；在非工作日，工厂停止生产，工作人员处于休息阶段，这时候工厂用电负荷处于低谷，居民生活和餐饮、服务行业的用电负荷则显著上升。

图 3.4 是某用户一天 24 小时的用电负荷变化曲线图，可以看到这 24 小时内用电负荷一直处于变化状态。从 0 点到 7 点之间，大部分用户处于休息睡眠状态，因此用电负荷处于较低水平且处于相当稳定状态，变化不是很大；从 7 点到 9 点用电负荷迎来第一波峰值，用户结束睡眠状态起床准备早饭、上班等相关事宜，电力需求上升；从 9 点到 12 点用电负荷开始下降，并在 12 点左右达到第二个用电高峰，这对应用户上班后回家，在家做午饭或午休的过程；从 12 点到 17 点后用户开始下午的工作日程，用电负荷再次保存在稳定的低谷状态；下午下班后用户回家制作晚餐并开始看电视等娱乐活动，对用电负荷的需求剧增，在 17 点到 20 点区间达到该日用电最高峰值；最后在 20 点到 23 点，人们结束其他活动开始准备休息，用电负荷逐渐下降至低耗电状态。

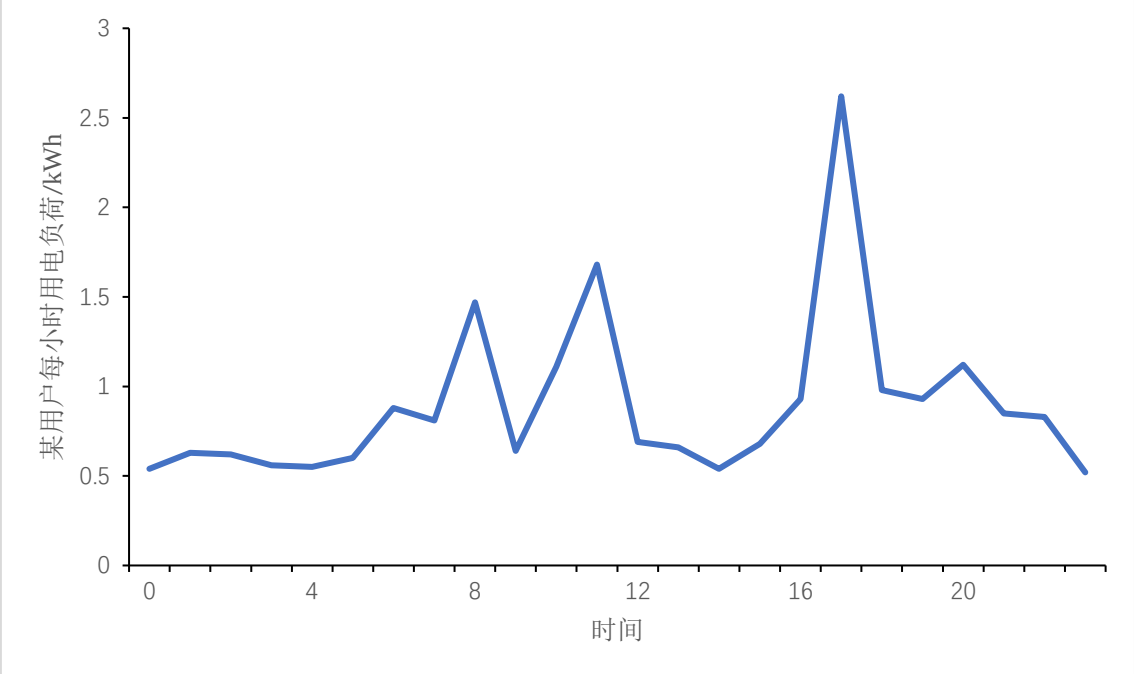


图 3.4 用电负荷日变化曲线
Fig.3.4 Daily load curve

图 3.5 是某用户一周 7 天的用电负荷变化曲线图，可以看到一周内每天的用电负荷变化趋势大致相同，在每天的相近时间都有相同的峰值、谷值出现；此外在周末也就是最后两天出现一周内用电负荷的最高值，这是由于周末非工作日用户在家进行丰富的娱乐活动或其他休闲活动导致的用电需求的上升。通过上述的相关分析，可见居民用电负荷同用户生活作息规律相关，而用户生活作息每天都大致相同，这就验证了前面所说大多数用电家庭表现出的是日周期特性。

中国知网 https://www.cnki.net

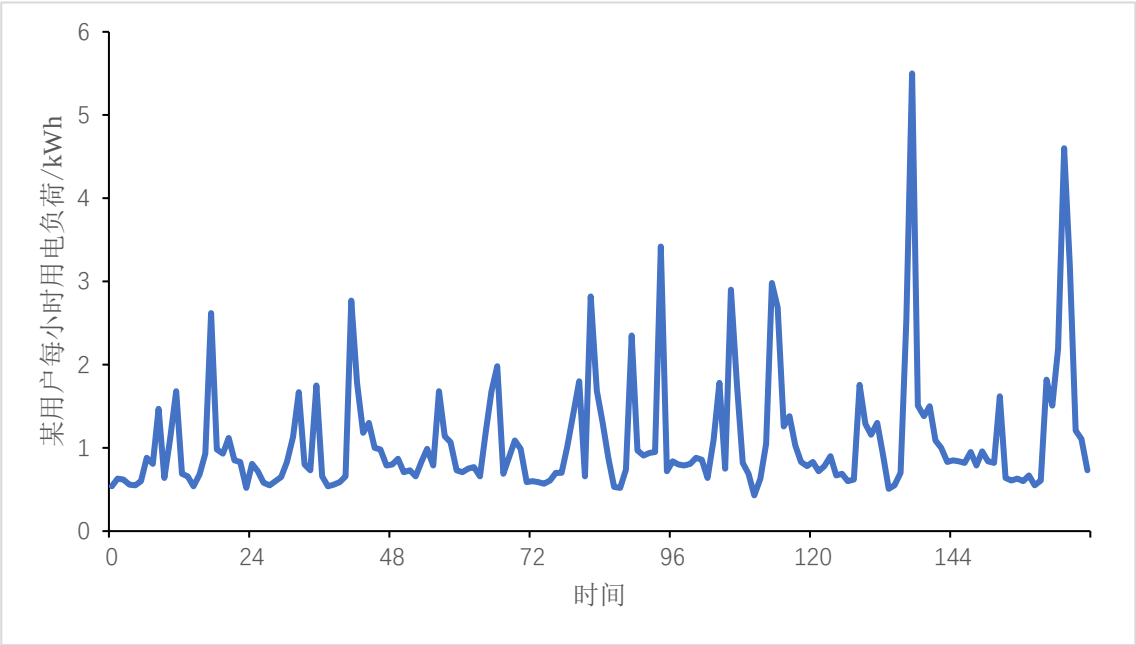


图 3.5 用电负荷周变化曲线
Fig.3.5 Weekly load curve

3.4 实验设计

3.4.1 数据预处理

实验中使用的数据集是“HUE:不列颠哥伦比亚省建筑物每小时能源使用”数据集。目前数据集中有 22 个家庭，大多数都有 3 年的电力消费历史。为了获得尽可能多的同期用电量数据，这里将时间段限定在“2015-08-21”到“2018-01-29”之间。根据这一规则，从中选择了 id 为 3-6、8-14 和 18-20 的房屋，共 14 个家庭。

在选择适当的数据之后，需要对数据进行预处理操作。基于数据驱动的深度学习负荷预测模型需要真实完整的负荷数据输入才能学习到负荷变化的内部规律，但在实际历史负荷数据的采集过程中可能存在人员采集错误、数据传输干扰、电力设备自身故障、存储丢失等问题，因此在数据集中会存在大量的缺失值和异常值[80]。神经网络对输入的训练数据十分敏感，异常数据会影响到神经网络的正常训练，如果不加处理就输入异常数据可能导致网络无法收敛。因此在对模型进行训练前很有必要对原始数据进行预处理操作。

（1）缺失值处理

在实际实验环境中，数据集存在缺失值的情况较为普遍，这通常会给机器学习系统带来很大问题。如果忽视缺失值，有些算法可能无法处理，致使模型触发异常；直接删除缺失值则可能导致模型性能下降甚至无法收敛。因此，处理缺失值被认为是提升整体

中国知网 https://www.cnki.net

数据质量的关键步骤。对于该数据集中的缺失值，这里使用缺失值附近的均值或插值对其进行填充处理，可以描述为：

$$x_i = \begin{cases} \dfrac{x_{i-1} + x_{i+1}}{2}, & x_i \in \text{Null}, x_{i-1}, x_{i+1} \notin \text{Null} \\ 0, & x_i \in \text{Null}, x_{i-1} \text{ or } x_{i+1} \in \text{Null} \\ x_i, & x_i \notin \text{Null} \end{cases} \tag{3.10}$$

其中x_i表示一段时间内的电力负荷数据。

（2）异常值处理

异常值又称离群点，是指数据集中存在不合理的个别值，其值与样本的其余观测值有显著差异。造成这种情况的原因很多，可能是电网正常运行时因突发性事件导致的负荷突然激增或陡降的情况，也可能是数据收集或数据传输过程中出现问题或其他原因。异常值会降低数据质量，并对模型性能产生不利影响。对异常值的处理一般有两个步骤，一是对异常值的识别，二是对异常值进行修正。本文采用常用的3σ准则来对异常值进行处理，具体公式如下：

$$f(x_i) = \begin{cases} \text{avg}(x) + 2 \cdot \text{std}(x) & \text{if } x_i > \text{avg}(x) + 2 \cdot \text{std}(x) \\ x_i & \text{otherwise} \end{cases} \tag{3.11}$$

式中，x表示由某一用户的采样计量值所组成的向量，$\text{avg}(x)$表示x的平均值，$\text{std}(x)$表示x的标准差。

（3）归一化处理

不同量纲的数据如果不经处理直接在模型中进行训练可能会影响模型的训练速度，也可能会影响模型的预测精度。数据归一化是指对数据集进行等比例缩放至[0,1]范围之间，对数据进行归一化操作，可以有效去除量纲的影响，将有量纲的数值变成无量纲的纯数值，解决各特征之间数值差异过大的问题，同时也可以减少数据的噪声，提升训练速度，防止过拟合。这里选择最大-最小缩放法对负荷数据进行归一化来平滑收敛。具体公式如下所示：

$$f(x_i) = \frac{x_i - \min(x)}{\max(x) - \min(x)} \tag{3.12}$$

式中，$\min(x)$和$\max(x)$分别表示向量x中的最小值和最大值。

图 3.6 和图 3.7 为某用户在某一时间区间的用电负荷曲线和它归一化后的数据表现。从两图对比中可以看出，原始数据和归一化后的数据变化走势完全相同，归一化后的数据都在[0,1]区间范围内。

中国知网 https://www.cnki.net

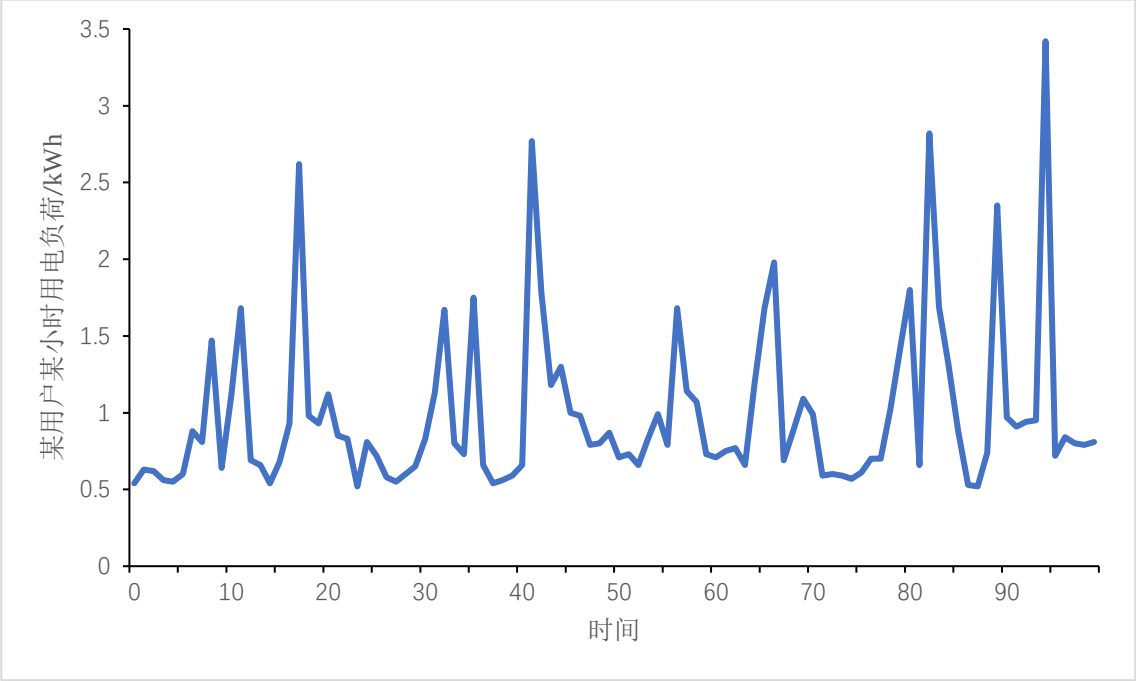


图 3.6 原始负荷数据
Fig.3.6 Raw load data

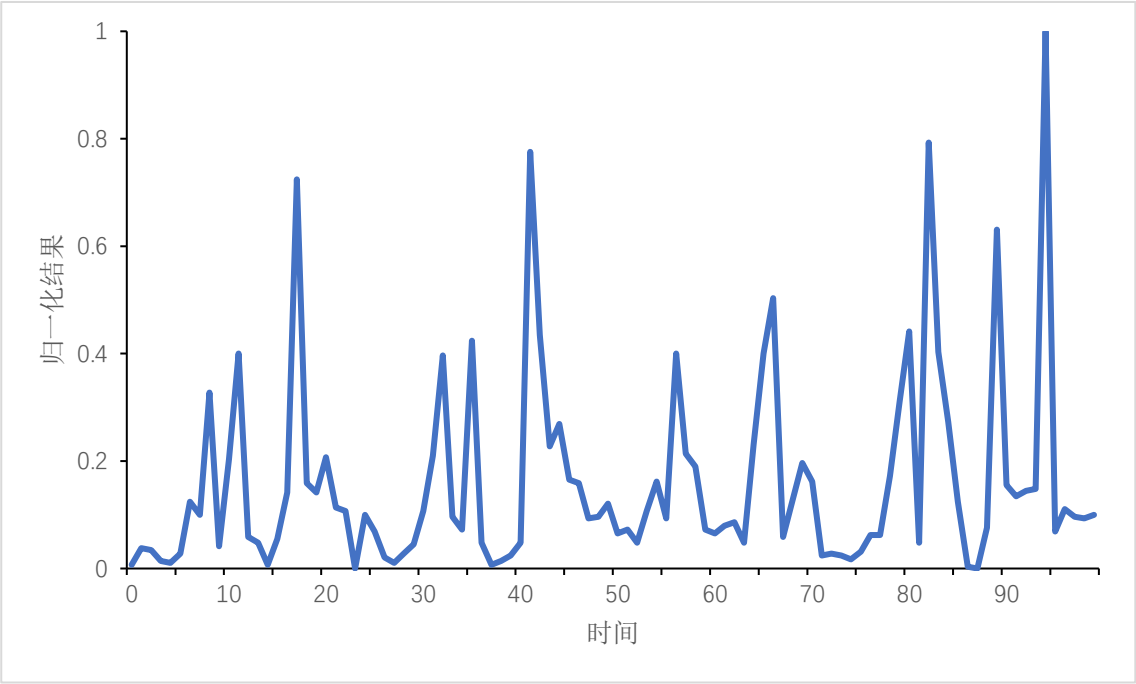


图 3.7 负荷数据归一化结果
Fig.3.7 Normalized load data

最后，将归一化处理过的数据按0.6/0.2/0.2的分割比划分为训练、验证和测试数据集。

3.4.2 LSTM 模型设计

考虑到 LSTM 便于序列建模且具有长时间记忆能力，因此在本实验中使用 LSTM 网络作为预测模型。要精准的对居民用电负荷进行预测，不仅要选择适合的神经网络模型，

中国知网 https://www.cnki.net

还要优化模型的各项参数。选择合适的参数，可以有效的加快模型收敛速度，提高模型性能表现。下面对该 LSTM 模型涉及到的各项超参数选择进行详细介绍。

（1）输入维度（滑动窗口大小）设置

为满足 LSTM 模型的输入要求，这里需要对时间序列数据通过滑动窗口进行采样处理。实验所用的数据集是居民的每小时用电数据集，按 3.3.2 小节中对居民用电负荷进行的分析，可以发现居民用电负荷表现出较为明显的日周期特性，所以这里设置滑动窗口的大小$t = 24$：这意味前 24 小时的连续用电量数据将输入 LSTM 模型，预测模型会输出下一个小时的用电量预测值。此时，LSTM 模型的输入维度也被设置为 24。

（2）优化算法选择

深度学习的目标是通过不断迭代训练寻找到最优的网络权重，以此最小化损失函数，这本质上是一个优化问题，因此优化算法便是深度学习算法的学习机制。选择合适的优化算法可以快速准确的寻找到最优权重，当前用于深度学习的各种优化算法都是从梯度下降算法演变而来的。梯度下降法本质是沿着负梯度方向不断逼近目标函数的最小值，其网络更新公式如下：

$$\theta = \theta - \eta \cdot \nabla_\theta J(\theta) \tag{3.13}$$

梯度下降法的求解，就是先计算目标函数$J(\theta)$的梯度$\nabla_\theta J(\theta)$，然后将待优化参数θ向负梯度方向更新（即公式 3.13），η为学习率，表明梯度更新的步伐大小。梯度下降法在每次更新梯度的时候，采用整个训练集的数据来计算损失函数对参数的梯度，所以计算非常缓慢，数据集规模大时表现更为明显。而且后续也不能加入新数据来实时更新模型。后续提出的随机梯度下降法（Stochastic Gradient Descent，SGD）在每次更新时对同一批内每个样本进行梯度更新，这样网络更新参数速度很快。而且 SGD 算法已经在联邦学习框架广泛应用，因此本文采用 SGD 优化算法。

（3）隐藏层设置确定

LSTM 隐藏层的设置主要包括隐藏层层数设置、神经元个数设置和激活函数设置，我们通过网格搜索方式对这些模型参数进行优化。这里设置一个简单的负荷预测任务来测试不同参数设置下的模型性能表现，并借此选择出最优参数。在 HUE 数据集中随机选择 3 户居民在 2015 年 8 月 21 日到 2017 年 8 月 21 日两年的历史用电负荷数据作为训练集对不同参数设置的 LSTM 模型进行训练，再将训练好的模型对这 3 户居民 2017 年 8 月 22 日的 24 小时用电负荷进行预测，计算它们的平均性能表现，以此来选择出最优参数设置。网格搜索完成后选出的最优隐藏层设置如表 3.2 所示。

中国知网 https://www.cnki.net

表 3.2 LSTM 的隐藏层设置

Tab.3.2 LSTM hidden layer settings

模型	超参数	搜索空间	最优值
LSTM	隐藏层数量	[1,2,3,4]	2
	隐藏层 1 神经元个数	[16,32,64,128,256]	128
	隐藏层 2 神经元个数	[16,32,64,128,256]	256
	激活函数	[relu,sigmoid,tanh]	relu

（4）损失函数确定

损失函数是模型预测值与真实值间差距的度量标准，可以用来指导模型参数的更新优化。不同的机器学习任务往往选择不同的损失函数，负荷预测任务属于回归问题，因此选择均方误差（Mean square error，MSE）来作为本实验的损失函数，其计算公式为

$$\mathrm{MSE}=\frac{\sum_{i=1}^{N}(y_i-\hat{y}_i)^2}{N} \tag{3.14}$$

其中，N代表数据集的样本数量，y_i，$\hat{y}_i$分别代表数据集上第i个样本的真实值和预测值。

至此 LSTM 模型的参数设置已经完成，具体情况如表 3.3 所示。

表 3.3 LSTM 的最优超参数

Tab.3.3 The optimal hyperparameters of LSTM

超参数	参数设置
输入维度	24
隐藏层层数	2
隐藏层 1 神经元个数	128
隐藏层 2 神经元个数	256
优化算法	SGD
激活函数	Relu
损失函数	MSE

3.5 实验与分析

3.5.1 实验环境

本仿真在实验室工作站上进行，其 CPU 为 Intel(R) Xeon(R) W-2255，GPU 为 NVIDIA GeForce RTX 3090，内存为 32GB。本案例在阿里巴巴集团开发的 FL 综合平台 FederatedScope[81]上运行，Python 版本为 3.9。

3.5.2 联邦参数设置

中国知网 https://www.cnki.net

按照 3.2 节所述的模型训练流程，本文提出的基于个性化联邦学习的负荷预测方法的联邦参数设置如下表 3.4 所示。

表 3.4 联邦学习参数设置

Tab.3.4 Federated learning parameter settings

超参数	值
客户的本地训练周期数	5
总通信轮数	500
每一轮参与计算的客户占比	0.3
隐私预算	2,4,6,8,10
批处理大小	128
学习率	0.0001

3.5.3 模型评估指标

电力负荷预测任务本质上属于回归问题，均方根误差（root Mean square error, RMSE）是回归问题中经典的评价标准，因此在本实验中采用 RMSE 作为评估标准，如公式 3.15 所示。RMSE 值越小，就说明模型的预测性能越好。

$$\mathrm{RMSE} = \sqrt{\frac{\sum_{i=1}^{N} (y_i - \hat{y}_i)^2}{N}} \tag{3.15}$$

其中，N代表数据集的样本数量，y_i和$\hat{y}_i$分别代表数据集上第i个样本的真实值和预测值。

3.5.4 实验结果与分析

（1）个性化负荷预测的性能表现

为了证明所提方法的优越性，这里对比了不同基准模型在该数据集上的预测性能。这些模型包括使用 FedAvg（Global）的传统全局模型，只使用 Ditto 框架的 PFL（PFL），带 DP 算法的 PFL（PFL-DP），以及本文提出的方法（PFL-GANDP）。表 3.5 显示了这些基准模型在 14 个客户负荷数据上的评估表现。这里采用基于拉普拉斯机制的 DP，其中 $\varepsilon = 6$。对比 PFL 和 Global 的预测表现，可以明显看出每个客户端下使用 PFL 的预测表现都要强于 Global，这说明了个性化策略在预测用户级负荷方面的优秀表现。对 PFL、PFL-GANDP 和 PFL-DP 的预测表现进行对比，可以看到使用差分隐私算法的 PFL-GANDP 和 PFL-DP 的 RMSE 值要高于 PFL，这表明差分隐私算法引入噪声提升了隐私保障，却也对预测性能造成了影响；对比 PFL-GANDP 和 PFL-DP 的预测表现，可以看到 PFL-GANDP 的预测性能要优于 PFL-DP，这表明使用的 GAN-DP 算法可以更好的平衡数据效用和隐私保护，PFL-GANDP 的预测表现已经接近甚至优于 Global 下的相关表

中国知网 https://www.cnki.net

现。

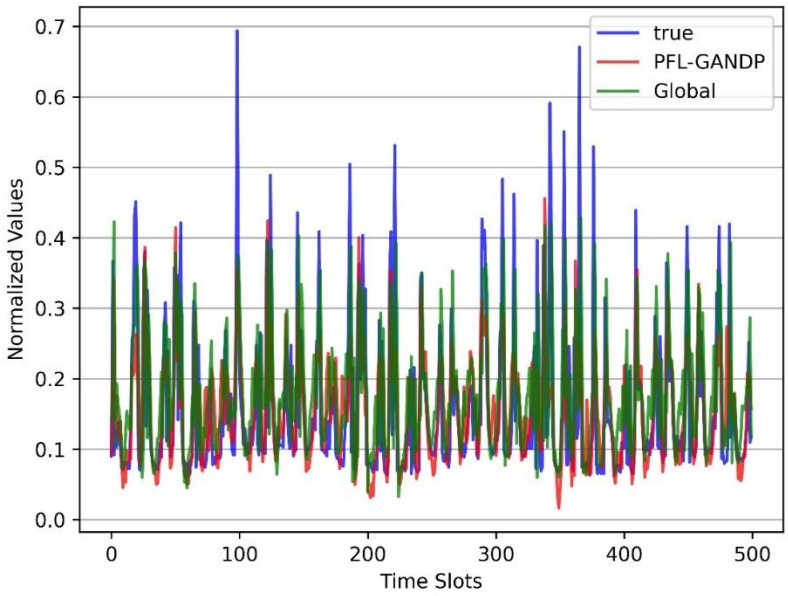
表 3.5 在 14 个用户使用不同模型的评估表现

Tab.3.5 Test loss(RMSE) for 14 customers using different model

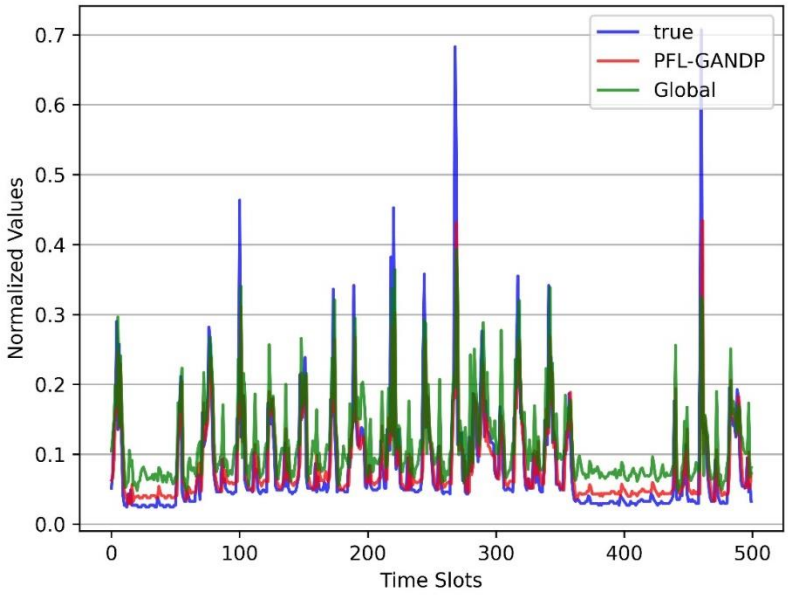
House id	Global	PFL	PFL-DP	PFL-GANDP
3	0.1991	0.1123	0.2388	0.2033
4	0.1406	0.0813	0.1930	0.1342
5	0.1465	0.0806	0.2251	0.1335
6	0.1046	0.0595	0.1774	0.1114
8	0.1532	0.0867	0.1832	0.1546
9	0.1192	0.0665	0.1875	0.1069
10	0.1338	0.0777	0.1788	0.1259
11	0.1345	0.0766	0.2042	0.1278
12	0.0926	0.0528	0.1583	0.1034
13	0.1466	0.0847	0.1890	0.1370
14	0.1077	0.0628	0.1443	0.1169
18	0.1821	0.1043	0.2679	0.1655
19	0.1593	0.0896	0.1997	0.1684
20	0.1410	0.0791	0.2312	0.1312

这里用随机选择的三个客户的测试数据集来对这些模型性能进行直观展示。图 3.8 展示了客户 1、4 和 7 使用全局模型 Global 和 PFL-GANDP 模型的预测结果。相比之下，可以看出所提方法的预测值更符合实际值。尽管全局模型在特定用户上的预测表现不佳，但仍有可以应用全局模型的新场景。这里将这 14 个客户的数据整合成一个区域用电数据集并对该数据集进行预测，可以看到全局模型可以在区域用电数据上进行有效预测，预测结果如图 3.9 所示。这意味着所提方法集成了全局和个性化模型，可以更好地服务于负荷预测场景。

中国知网 https://www.cnki.net

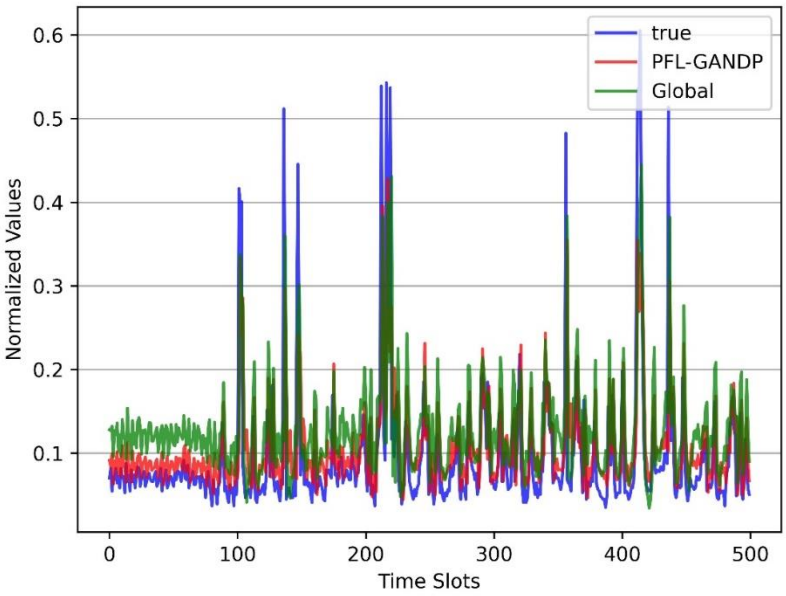


(a) client 1



(b) client 4

中国知网 https://www.cnki.net



(c) client 7

图 3.8 使用全局模型和所提模型预测电力负荷的结果

Fig.3.8 Forecasting results for electrical load using global and our proposed model.

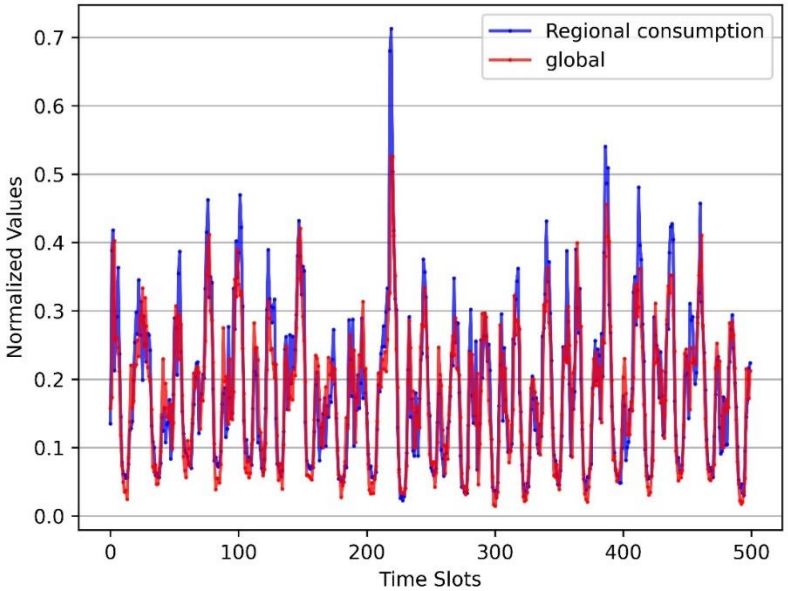


图 3.9 采用全局模型预测区域用电负荷结果

Fig.3.9 Forecasting results for electrical load on regional consumption using global model

（2）与传统 DP 策略的比较

此外，本文还进行了相关实验来证明所提系统在隐私保护方面的优越性。在图 3.10 中比较了 PFL-GANDP 和 PFL-DP 在不同隐私预算ε下的预测性能。横向上，随着隐私预算的增加，添加的噪声减少，RMSE 值都在降低，说明两种模型的预测精度也有所提

中国知网 https://www.cnki.net

高。通过纵向比较，在相同的隐私预算下，所提系统 PFL-GANDP 能够实现比 PFL-DP 更好的预测性能，这意味着 GAN-DP 能够在隐私保护和预测性能之间实现更好的权衡。图 3.11 提供了这两种模型在用户数据集上的预测性能的可视化表示。可以看到所有模型都可以通过偏离蓝色实线(真实数据)来提供隐私保护。

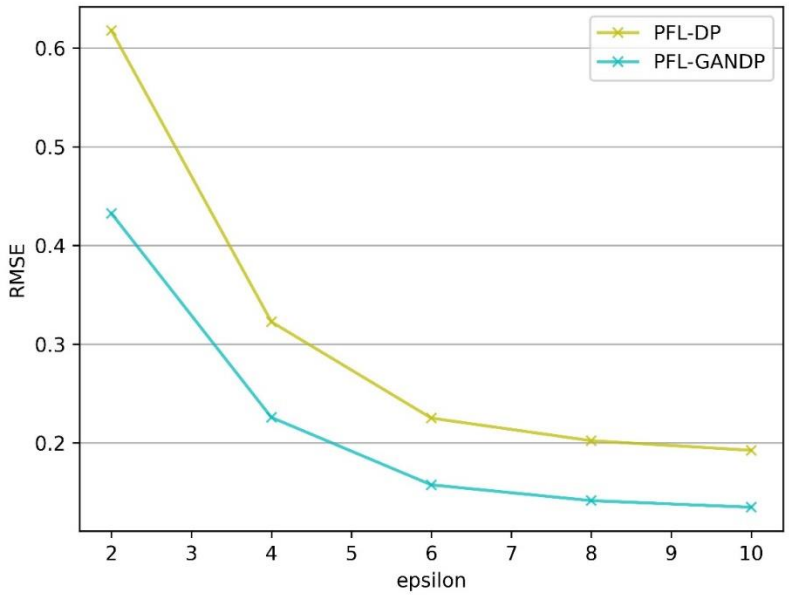


图 3.10 隐私保护效果对比

Fig.3.10 Comparison of privacy protection effect

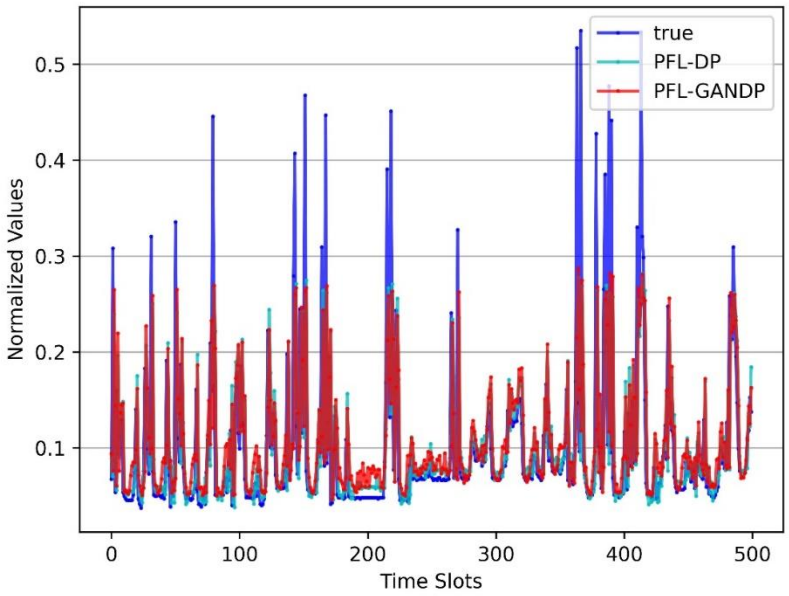


图 3.11 在隐私保护策略下预测表现

Fig.3.11 Forecasting performance on privacy protection strategy

中国知网 https://www.cnki.net

3.6 本章小结

在本研究中提出了一个基于个性化联邦学习的用户级负荷预测系统，用户可以通过个性化模型进行定制预测，同时得到的全局模型可以有效预测区域用电数据，拓宽了负荷预测系统的应用场景。后面进一步应用 GAN-DP 来增加系统的隐私保护性能，同时最大限度地减少对预测精度的影响。实验结果表明，所提方法能够准确地预测用户级负荷并保护隐私。

中国知网 https://www.cnki.net

第四章 基于 one-shot 联邦学习的高效负荷预测方法

4.1 引言

基于联邦学习的负荷预测方法通过联邦聚合对全局模型进行训练，该方法只发送模型参数，不共享原始数据，使得私人用电数据可以安全保留本地。在第三章的工作已经初步展示了基于个性化联邦学习的负荷预测方法的优秀性能。

本章对基于联邦学习的负荷预测任务进行更深层的思考，发现高通信开销问题阻碍着现实场景下联邦学习的进一步发展。一方面，随着智能手机等移动设备数量的迅猛增长和硬件的不断更新迭代，用户端算力有所加强，但由于现有的基础设施不够完备，导致运营商无法提供可靠廉价的网络连接服务。另一方面，部署在移动设备上的高级机器学习应用程序越来越多地使用复杂的深层神经网络，以至于每个参与训练的客户端上传的模型参数更新需要占用更大的带宽，使得通信问题成为限制联邦学习发展的瓶颈。因此，最大限度地减轻联邦学习中的通信开销变得尤为重要。

针对这一问题，我们设计了一种基于单次联邦学习（one-shot FL）的高效负荷预测方法。该方法面向负荷预测场景，通过数据集蒸馏算法对训练数据进行蒸馏，这样整个联邦学习过程中客户端仅需向服务器进行单次通信来传输蒸馏数据，最终在蒸馏数据上进行模型训练，完成用户负荷预测任务。在大幅降低通信成本的同时，该联邦学习框架使用蒸馏数据来代替梯度进行传输，整个单次通信过程不涉及模型训练中的梯度更新信息，避免了由梯度泄露反推私人数据集的可能，以此大大降低了客户端数据隐私泄漏的风险。

4.2 方法介绍

这一节介绍本章的主要方法。受数据集蒸馏算法的启发，我们设计了一种基于单次联邦学习的高效负荷预测方法。不同于传统联邦学习下客户端和服务器间的多轮次通信，该方法只需要客户端和服务器之间进行单次通信就能保证训练表现。每个客户端对本地原始数据进行蒸馏，并将得到的蒸馏数据和学习率（取代传统的梯度或权重）上传到服务器，在服务器上进行数据聚合后完成模型训练。

4.2.1 数据集蒸馏基本流程

数据集蒸馏算法的关键思想是使用梯度下降来学习出原始数据集上对快速训练神经网络最有帮助的特征。数据集蒸馏通过从大型训练数据中学习出一小组蒸馏信息，构建出规模更小且有含有相当信息量的合成数据集。传统深度模型训练需要在原数据集上进行上百次训练才能达到一定性能，相比之下使用少量的蒸馏数据就能实现模型的快速

中国知网 https://www.cnki.net

收敛，这大大提升了网络训练效率。

首先介绍下基本的神经网络训练过程。假定有这样一个训练数据集$\mathbf{X}=\{x_i\}_{i=1}^{N}$，$N$为数据个数。将神经网络参数预设为$\theta$，并用$\ell(x_i,\theta)$来表示该网络在数据点$x_i$上的损失函数。这样训练任务目标就是找到使整个训练数据的经验损失最小时的神经网络参数θ^*：

$$\theta^*=\arg\min_{\theta}\frac{1}{N}\sum_{i=1}^{N}\ell(x_i,\theta)\triangleq\arg\min_{\theta}\ell(\mathbf{X},\theta) \tag{4.1}$$

需要注意的是，这里为了简化符号，对$\ell(\cdot)$符号重新进行了定义，$\ell(\mathbf{X},\theta)$表示整个数据集上θ的平均误差。同时假设ℓ是二次可微的，保证其适用于机器学习任务。

通过标准训练寻找最优解θ^*通常采用小批量随机梯度下降的方法。在第t轮训练时，一个小批量训练数据$\mathbf{X}_t=\{x_{t,j}\}_{j=1}^{n}$（训练数据集$\mathbf{X}$的子集）被采样用来为当前参数$\theta_t$进行更新：

$$\theta_{t+1}=\theta_t-\eta\nabla_{\theta_t}\ell(\mathbf{X}_t,\theta_t) \tag{4.2}$$

式中η为学习率。标准情况下需要上千次参数更新模型才能收敛。

不同于上述的一般情况，对于数据集蒸馏的训练过程，在给定模型和数据集时，数据集蒸馏的目标是获得一个蒸馏的合成数据集$\tilde{\mathbf{X}}=\{\tilde{x}_i\}_{i=1}^{M}$（其中$M\ll N$）和相应的学习率$\tilde{\eta}$，保证在合成集上训练的模型与在原始数据集上训练的模型的测试精度不相上下。

值得注意的是，数据集蒸馏要在原始数据集上的性能仍然保留足够的任务相关信息，以便在其上训练的模型可以泛化到未见的测试数据。因此，蒸馏算法必须在大量压缩信息和不完全消除信息间达到微妙的平衡[82]。

给定初始化参数θ_0，使用合成数据$\tilde{\mathbf{X}}$进行单步梯度下降，对网络参数进行更新的过程可以表示为：

$$\theta_1=\theta_0-\tilde{\eta}\nabla_{\theta_0}\ell\left(\tilde{\mathbf{X}},\theta_0\right) \tag{4.3}$$

这样通过最小化$\mathcal{L}(\cdot)$来获得这些合成数据$\tilde{\mathbf{X}}^*$和学习率$\tilde{\eta}^*$：

$$\tilde{\mathbf{X}}^*,\tilde{\eta}^*=\arg\min_{\tilde{\mathbf{x}},\tilde{\eta}}\mathcal{L}\left(\tilde{\mathbf{X}},\tilde{\eta};\theta_0\right)=\arg\min_{\tilde{\mathbf{x}},\tilde{\eta}}\ell(\mathbf{X},\theta_1)=\arg\min_{\tilde{\mathbf{x}},\tilde{\eta}}\ell\left(\mathbf{X},\theta_0-\tilde{\eta}\nabla_{\theta_0}\ell\left(\tilde{\mathbf{X}},\theta_0\right)\right) \tag{4.4}$$

接下来，关于$\tilde{\mathbf{X}},\tilde{\eta}$，可以使用基于梯度的标准方法进行优化求解。

4.2.2 基于 one-shot 联邦学习的高效负荷预测方法

（1）联邦学习下的数据蒸馏

受数据集蒸馏算法的启发，本文提出了一种基于数据集蒸馏的单次联邦学习来进行居民负荷预测来显著降低通信成本，同时还要保证一定的性能表现。要将数据集蒸馏算法应用于联邦学习中，需要考虑蒸馏数据集是否可以代替传统联邦学习下的权重或梯度

中国知网 https://www.cnki.net

进行传输通信。通过上一小节的了解可以得知，内容上蒸馏数据集虽然压缩了规模，但学习到了原始数据集的鲜明特征，其数据信息足以满足全局模型的训练要求；在隐私保护方面由于数据集蒸馏算法开始进行的是随机初始化，且蒸馏数据集在规模上要远小于原始数据集，两者不存在明显的函数关系。可以证明的是[83]，数据集蒸馏产生的合成数据集是由特定的模型权重分布生成的，在模型更新后变得无用。在不知道服务器分配的初始权重的情况下，攻击者无法使用泄漏的蒸馏数据推导出全局模型。

以联邦学习设置中第k个客户端为例，该客户端进行本地数据集蒸馏的算法伪代码如下：

算法 2：本地数据蒸馏

输入：第k客户端的本地数据集$\boldsymbol{X}_k$

超参数：蒸馏数据个数M，初始化模型参数θ_0，初始化学习率η_0，步长α，批数据大小n，训练轮次T。

1：对蒸馏数据集和学习率进行随机初始化 $\tilde{\boldsymbol{X}}_k = \{\tilde{x}_i\}_{i=1}^{M}$，$\tilde{\eta} = \eta_0$

2：**for** 每一训练轮次$t = 1\ to\ T$ **do**

3：　　从本地数据集$\boldsymbol{X}_k$中选取大小为n的子集 $\boldsymbol{X}_{kt} = \{x_{t,j}\}_{j=1}^{n}$

4：　　使用梯度下降来更新模型参数，得到θ_1

5：　　评估新模型参数在真实训练数据子集上的损失表现 $\mathcal{L} = \ell(\boldsymbol{X}_{kt}, \theta_1)$

6：　　对蒸馏数据集和学习率进行更新：$\tilde{\boldsymbol{X}}_k = \tilde{\boldsymbol{X}}_k - \alpha\nabla_{\tilde{X}_k}\mathcal{L}$，$\tilde{\eta} = \tilde{\eta} - \alpha\nabla_{\tilde{\eta}}\mathcal{L}$

7：**end for**

输出：蒸馏数据集$\tilde{\boldsymbol{X}}$；学习率$\tilde{\eta}$

在联邦学习场景下，这里经由数据集蒸馏方法压缩各客户端的原始数据集，合成的蒸馏数据规模大大降低的同时保留了客户数据的特征信息。在联邦学习中使用蒸馏数据代替模型参数进行通信可以显著降低通信开销。

（2）单次联邦学习算法设计

假设有编号为$1, \dots N$的客户端，每个客户端各有自己的本地模型$f_{\theta_1}, \dots, f_{\theta_N}$，对应的模型参数$\theta_1, \dots, \theta_N$，损失函数 $L_1, \dots, L_N$。给定某个概率向量$p = (p_1, \dots, p_N)$，（$0 \le p_k \le 1$，$\sum_k p_k = 1$），目标是要找到模型参数θ^*，使加权和最小，即

$$\theta^* = \arg\min_{\theta} \sum_{k=1}^{N} p_k L_k(\theta) \tag{4.5}$$

因此，对于每个客户端$k = 1, \dots N$与数据集$\boldsymbol{X}_k$，$L_k(\theta) = \ell(\theta; \boldsymbol{X}_k)$，本文所提单次联邦学习算法主要包括以下三个步骤。

1）中心服务器初始化模型参数θ_0。

2）各客户端对它们的本地数据集进行蒸馏。这里首先初始化蒸馏数据$\tilde{x}$,、蒸馏标签

中国知网 https://www.cnki.net

$\tilde{y}$,和相应的学习率$\tilde{\eta}$。$\tilde{x}$中的每一项都是从标准正态分布中提取的，而$\tilde{\eta}$设为预定义值η_0。针对负荷预测任务，这里提取的标签初始化为回归问题的正态分布随机向量。在真实数据集上通过梯度下降更新模型参数θ_1使损失降至最低。

$$\theta_1 = \theta_0 - \tilde{\eta}\ell(\theta_0; \tilde{x}, \tilde{y}) \tag{4.6}$$

在重复蒸馏预定次数后获得蒸馏数据集$\{(\tilde{x}_j, \tilde{y}_j, \tilde{\eta}_j)\}$。

3）各客户端将蒸馏数据上传到服务器上组合为蒸馏数据集。然后服务器在该数据集上训练全局模型。

算法 3 对这些步骤进行了总结。

算法 3：基于数据集蒸馏的 one-shot 联邦学习算法

1：初始化模型参数θ_0
2：**for** 每一个参与训练的客户 **do**
3：　　数据集蒸馏
4：　　把蒸馏数据发送给服务器
5：**end for**
6：服务器聚合各客户端的蒸馏数据集
7：服务器在聚合后的蒸馏数据集上进行集中训练，通过随机梯度下降对θ^*进行更新
8：将全局模型θ^*广播给各客户端进行预测

在该算法中，全局模型的训练不在依赖于传统联邦学习下多次传输的模型参数更新，而是经由蒸馏数据的单次通信传输来实现的，客户端与服务器间大大减少了通信成本，相应的各客户端和服务器有了额外的计算成本。

（3）一种基于 one-shot 联邦学习的负荷预测方法设计

在上一小节中提出的单次联邦学习算法基础上，本文面向实际的居民负荷预测场景在标准联邦学习框架上进行了调整，提出一种基于数据集蒸馏的单次联邦学习负荷预测方法。这里输入为客户端数据（即用电住户），输出为服务器端（即电力公司）训练的全局模型θ^*，最后全局模型θ^*会广播给各客户端进行负荷预测。

其主体过程的描述如图 4.1 所示。

标准的联邦学习算法（以 FedAvg 为例）在全局模型的训练中需要进行多轮迭代才能收敛，这在很大程度上依赖于模型参数更新在客户端与服务器间的反复传输。当全局模型结构设置比较复杂，或是各客户端的本地数据异构现象严重时，模型想要收敛 FedAvg 就需要进行更多的迭代轮次，就会导致通信开销的进一步加剧。而本文所提方法传输的是蒸馏数据，这样可以有效避免重型模型或是数据异构带来的额外通讯负担，极大提高了通信效率。

中国知网 https://www.cnki.net

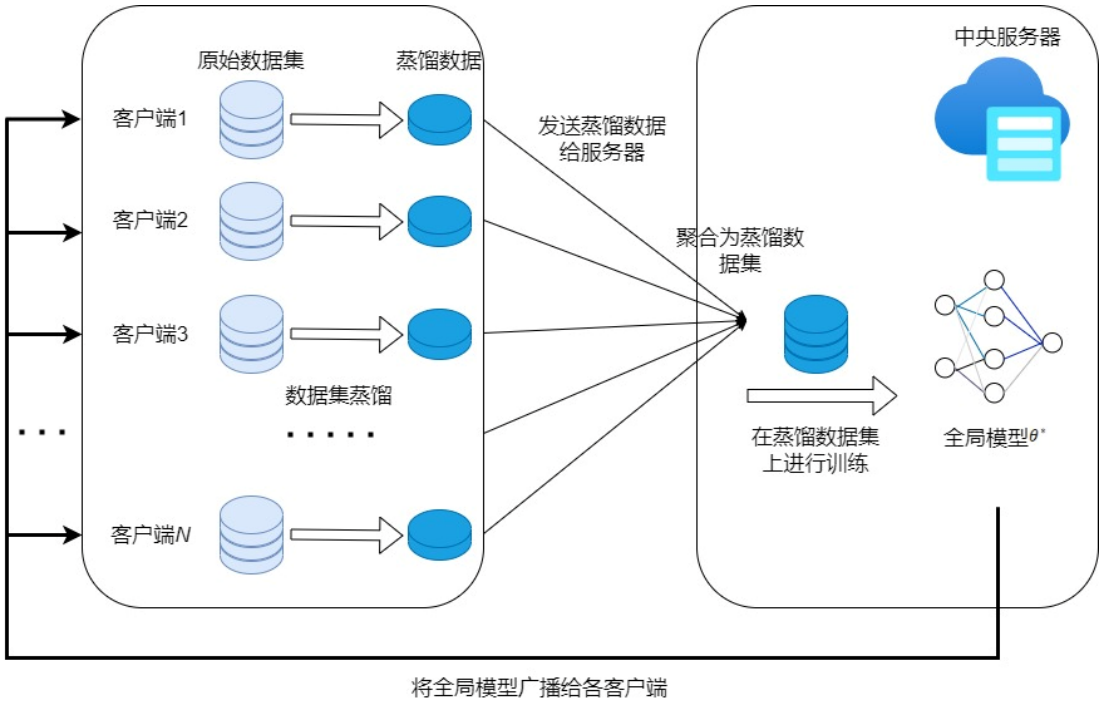


图 4.1 基于 one-shot 联邦学习的高效负荷预测框架

Fig.4.1 High efficiency load forecasting framework based on one-shot federated learning

在隐私保护方面，有相关研究[84]表明经由传统联邦学习通信中泄露的梯度信息可以反向推理出本地用户数据，简单的梯度共享模式存在一定的安全风险。在本文的算法中蒸馏数据代替梯度在客户端和服务器之间进行传输，后续全局模型在蒸馏数据集上进行训练，整个训练流程在服务器上进行不再涉及模型参数更新的传输，杜绝了由梯度泄露引发的用户隐私数据安全问题。

4.3 实验设置

本章在配备了 GeForce RTX 2080Ti GPU 的远程服务器上进行实验，各网络模型主要使用 python 语言中的 pytorch 库进行搭建。因为 LSTM 便于序列建模且具有长时间记忆能力，这里的用户用电负荷预测模型仍使用 LSTM 网络，所用 LSTM 网络的参数设置参考 3.4.2 小节的相关说明。

4.3.1 实验数据说明

本章采用数据集与第三章使用数据集相同，同为“HUE：不列颠哥伦比亚省建筑物每小时能源使用”数据集。数据集的预处理方法与 3.3.1 小节中采用的方法相同，首先采用插值法来填充数据中的缺失值，用3σ准则处理数据中的异常值，再用最大-最小缩放法对数据进行归一化操作。

同第三章相同，为了获得尽可能长的时间跨度，将时间段限定在“2015-08-21”到“2018-01-29”之间。根据这一规则，选择了 id 为 3-6、8-14 和 18-20 的房屋，共 14 个

中国知网 https://www.cnki.net

家庭。因为该数据集收集的是每小时的能源使用情况，所以每一客户对应的数据表现为一维数据。然后通过滑动窗口（$t = 24$）来处理数据，这里将用电数据从一维转换为二维数据，此时将数据集划分为 80%的训练集和 20%的测试集。

接下来对划分出来的训练集进行数据蒸馏操作。按照 4.2.2 一节中关于数据集蒸馏算法的实验设定，在蒸馏时各客户端采用当前全局模型进行本地模型初始化，数据集蒸馏时的超参数设置如下：蒸馏数据个数 M 取多段设置，令$M = 10,50,100$。初始化的学习率设置为 0.02，本地训练轮数设置为 10，批数据大小设置为 1024。此外，全局模型基于蒸馏数据集进行模型更新的轮数设置为 50。对数据集的处理流程如图 4.2 所示。

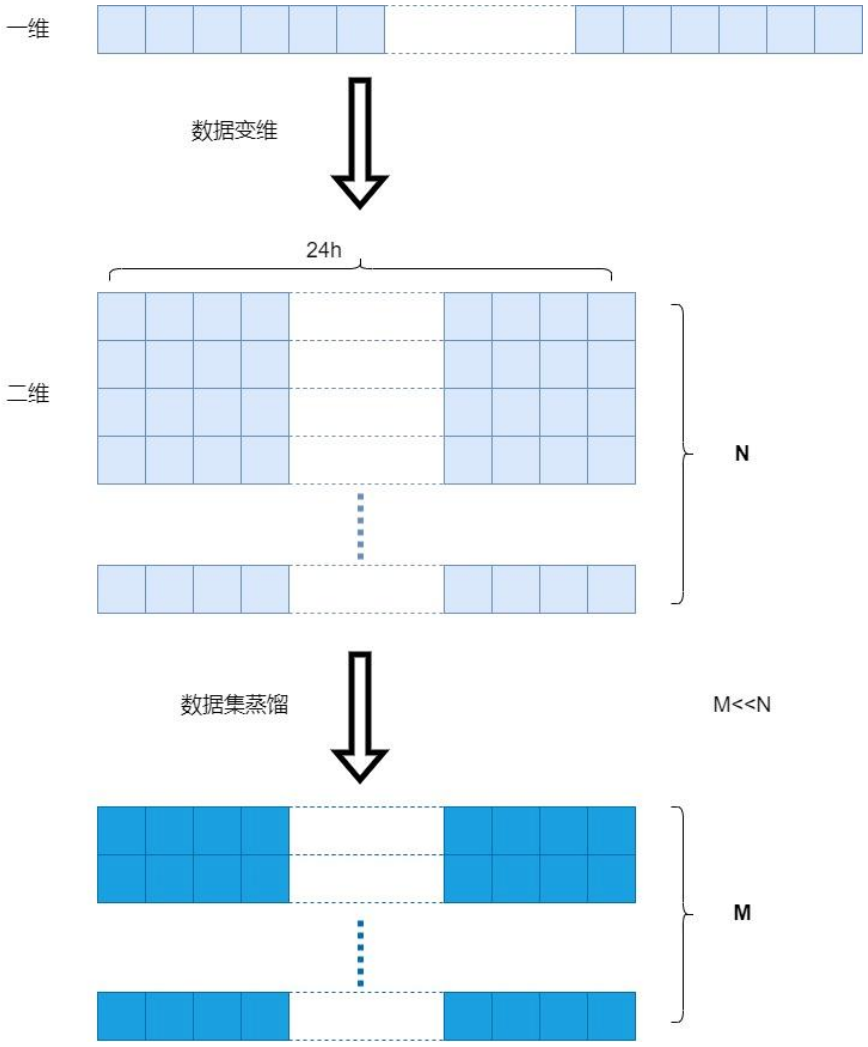


图 4.2 数据处理流程

Fig. 4.2 Data processing flow

4.3.2 实验评估指标

该实验评估指标主要包括模型性能评价指标以及通信效率评价指标。

由于本实验的训练任务为回归任务，因此选择经典的均方根误差（RMSE）作为模型性能的评价指标。RMSE 表示的是期望值与实际值之间的距离，当 RMSE 值越小，就

中国知网 https://www.cnki.net

说明模型的性能越好，预测的就越准确。

$$\mathrm{RMSE} = \sqrt{\frac{\sum_{i=1}^{N} (y_i - \hat{y}_i)^2}{N}} \tag{4.7}$$

其中，y_i为实际能耗测量值，$\hat{y}_i$为预测值，N为预测值总数。

对于通信效率评价指标，本文提出的方法大大提高了传统联邦训练产生的客户端和服务器间的通信效率，所以这里选择联邦学习过程中的客户端同服务器间的通信轮数以及总通信量作为评价指标。

4.4 评估分析

本章实验选择不同的模型作为对比方法，这些模型包括使用 FedAvg 的传统模型，集中训练模型（Centralized）以及本文提出的方法（one-shot FL）。接下来，以 RMSE 为模型评价指标，基于 4.3 节中的实验设置，通过实验观察上述框架在居民用电负荷数据上的预测表现。

在标准联邦平均学习 FedAvg 框架中，设置客户端参与训练比例$\mathrm{C} = 1$，即全部客户端参与全局模型训练。本地迭代设置为 3 次，全局迭代为 500 次，批数据大小设置为 128，学习率设置为 0.01，其中，客户端采用随机梯度下降 SGD 算法进行本地训练。

对于本文的 one-shot FL 框架，该框架与 FedAvg 框架均设置客户端数目为 14，其他联邦设置同 FedAvg 算法的实验设置相同。不同点在于 FedAvg 框架下客户端使用原始数据集参与训练，而 one-shot FL 框架则是由中央服务器使用蒸馏数据进行训练。

4.4.1 预测性能比较

首先对各框架在负荷数据上的预测性能进行比较。使用 one-shot FL 框架进行负荷预测时，这里将蒸馏数据个数取多段设置，令$M = 10,50,100$来看不同蒸馏数据规模对预测性能的影响。表 4.1 显示了这些基准模型在负荷数据上的评估表现，表格里的 RMSE 值为对应模型在各客户端评估表现的平均值。

表 4.1 不同基准模型下的负荷预测表现

Tab.4.1 Performance of load forecasting under different benchmark models

	one-shot FL			FedAvg	Centralized
	$M = 10$	$M = 50$	$M = 100$		
RMSE	0.2053	0.1610	0.1713	0.1772	0.1570

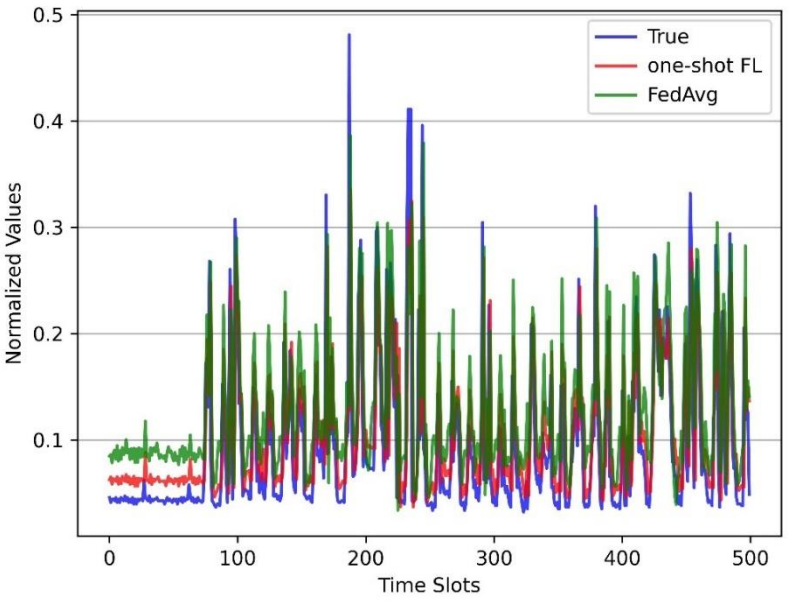
从上表中可以明显看出数据集蒸馏策略在用户负荷预测方面的优秀表现。相比于传统的 FedAvg，使用蒸馏数据的 one-shot FL 的 RMSE 值更低，这清晰地展示了模型性能的提升。针对M的变化趋势对预测性能的影响，可以看出蒸馏数据规模对模型性能的影

中国知网 https://www.cnki.net

响存在一个最优解，经过优化模型性能还能进一步提升。值得注意的是，当蒸馏数据规模取值较小时（$M = 10$）模型的性能表现反而变差。尽管该现象不是本文的研究内容，但对此有一个基本的猜想。数据集蒸馏的目标是一个小型的合成数据集，它需要保留足够的任务相关信息，以便在其上训练的模型可以泛化到未见的测试数据。因此，蒸馏算法必须通过大量压缩信息而不完全消除信息来达到微妙的平衡。出现这样性能下降的情况，有很大可能是压缩信息过度损失了部分重要特征，进而在进行预测时表现不佳。两种联邦学习框架 one-shot FL 和 FedAvg 的预测性能表现也可以通过预测图像来直观感受，这里随机选择了 2 个用户在 one-shot FL（$M = 50$）和 FedAvg 下的预测表现，并在图 4.3 进行展示。从图中可以直观看出本文所提模型的预测值更接近实际值。

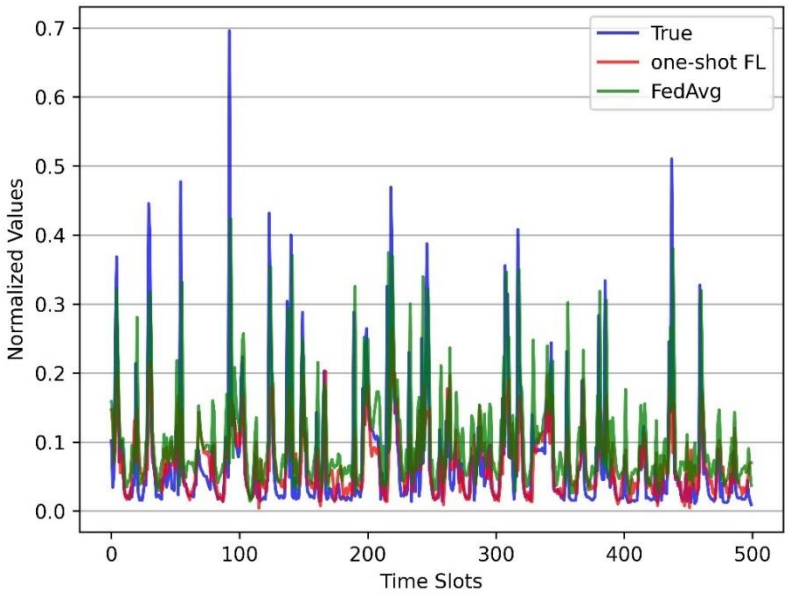
4.4.2 通信效率比较

相比于传统 FedAvg 需要多轮通信，one-shot FL 的突出优势在于仅需要服务器和客户端间的单次通信即可，并且蒸馏数据集的大小要小于参与更新的模型参数规模。按照 3.4 节中采用的 LSTM 网络设置，用于负荷预测的网络模型参数大小为 0.3MB。在 FedAvg 设置中，本文将各客户端向服务器上传模型更新，服务器向各客户端广播全局模型参数当做一个完整的通信轮次，所以一个客户同服务器之间的一次通信开销为 0.6MB。



(a) client 1

中国知网 https://www.cnki.net



(b) client 2

图 4.3 在不同框架下的预测表现

Fig.4.3 Predicted performance under different frames

one-shot FL 框架中使用蒸馏数据代替模型参数更新参与客户端和服务器间的通信，因此通信开销即表示为蒸馏数据集的规模。蒸馏数据集的大小与蒸馏数据的个数有关，参照 4.3 节中的数据处理流程，当蒸馏数据个数$M = 100$时，因为这里的时间窗口大小选取的为 24，所以单个客户端下的本地蒸馏数据集大小为 0.02MB。

这里对比 one-shot FL 框架和 FedAvg 在训练生成的模型达到相同的评价标准时，所需要的通信次数以及训练过程中的通信消耗。针对该负荷预测任务，文中设置预测模型的标准评估值 RMSE 为 0.20。在该设置下两种框架在通信次数和通信消耗上的比较如表 4.2 所示。

表 4.2 不同框架下的通信量对比

Tab.4.2 Comparison of communication traffic under different frames

框架	模型	通信次数	通信量（MB）
one-shot FL	LSTM	1	0.28
FedAvg		130	78

由表 4.2 可知，相比 FedAvg 框架，one-shot FL 大大降低了通信成本，通信节省高达 3 个数量级。因为传输通信的是蒸馏数据不涉及模型参数，所以随着模型增大，该框架的通信优势会更大。但需要注意的是虽然在通信开销节省上有着优异表现，但不可否认的是 one-shot FL 对客户端的本地算力要求有所增加，在实际部署时要考虑本地算力

中国知网 https://www.cnki.net

和通信开销的取舍情况。

4.4.3 隐私性能分析

联邦学习本身是隐私计算技术的一种，所以有必要对本文所提方法的隐私保护性能进行分析。但鉴于目前的研究还缺少相应的指标对基于数据集蒸馏的联邦学习过程的隐私保护程度进行评价，所以在这里定性分析下 one-shot FL 框架相比于 FedAvg 框架在隐私安全方面的进步。

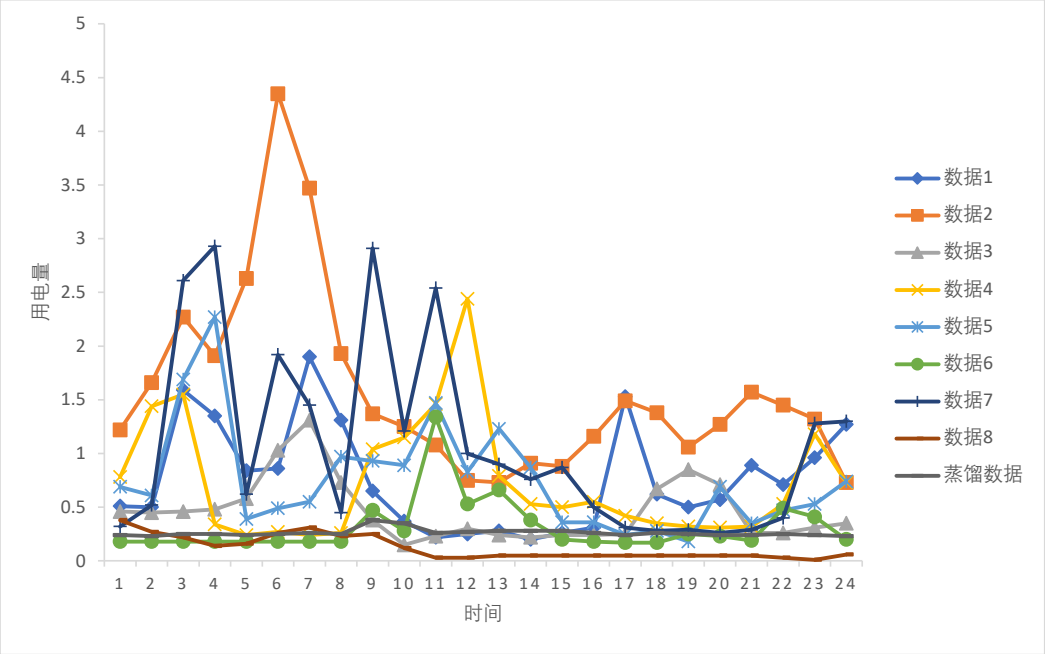


图 4.4 真实数据与蒸馏数据的对比

Fig.4.4 Comparison of real data with distilled data

图 4.4 显示了某一客户端 24 小时区间里真实数据和蒸馏数据的比对情况，在人眼看来，提取出来的序列是完全是随机的。因此，从蒸馏数据中提取信息的有效方法只能是通过泄露的蒸馏数据来训练目标模型。一方面，因为本文的 one-shot FL 框架仅有一次通信机会，极大减少了数据泄露可能；另一方面，由于蒸馏数据在训练时依赖特定的初始化，因此在泄露数据上训练不同初始化的模型会导致低精度模型。而且有数据集蒸馏的相关研究证明[75]攻击者无法在没有服务器初始权重的情况下借助蒸馏数据重新生成全局模型。综上所述，可以认为 one-shot FL 框架的隐私保护能力要强于 FedAvg。

4.5 本章小结

为应对负荷预测场景下联邦学习的高通信开销问题，本文从减少客户端和服务器的通信次数的角度出发，设计了一种基于单次联邦学习的高效负荷预测方法。将数据集蒸馏方法对用户原始数据集进行压缩，减小数据规模的同时也保留了原始数据特征。然后将蒸馏数据发送到服务器端进行组合，并在合成的蒸馏数据集上对全局模型进行训练。

中国知网 https://www.cnki.net

实验结果表明，所提出的预测方法通信成本要远低于传统方法，蒸馏数据也能有效的防止被窃听攻击者利用。

中国知网 https://www.cnki.net

中国知网 https://www.cnki.net

第五章 总结与展望

5.1 总结

居民用电负荷预测是电力数据挖掘中的一个重要研究方向，对于提高电网效率，保障社会稳定具有重要意义。为了进一步提升用户数据效用和保障用户数据隐私安全，本文研究了基于联邦学习的负荷预测方法，在个性化和高效通信两个方向都取得了良好的效果，并通过真实数据集进行了实验验证。本文的主要研究工作如下：

（1）针对现有的基于联邦学习的预测方法在数据异质性和隐私泄露方面的不足，本研究提出了一个基于个性化联邦学习的用户级负荷预测系统，用户可以通过个性化模型进行定制预测，同时得到的全局模型可以有效预测区域用电数据，拓宽了负荷预测系统的应用场景。然后进一步应用 GAN-DP 来增加系统的隐私保护性能，同时最大限度地减少对预测精度的影响。实验结果表明，所提方法能够准确地预测用户级负荷并保护隐私。

（2）高通信开销问题阻碍着现实场景下联邦学习的进一步发展，为此在数据集蒸馏算法的基础上，本文设计了一种基于单次联邦学习的高效负荷预测方法。该方法面向负荷预测场景，利用蒸馏数据的传输来完成客户端与服务器之间的单次通信。最终在蒸馏数据集上完成全局模型训练。该联邦学习框架在大幅降低通信成本的同时，使用蒸馏数据来代替梯度进行传输，避免了由梯度泄露反推私人数据集的可能，提供了额外的隐私保证。

5.2 展望

本文针对居民负荷预测任务，对基于联邦学习的负荷预测进行了改进和探索，取得了一些研究成果。但仍还有待深入和改进的地方，主要内容包括：

（1）两种改进方法的集成。本文的第三章、第四章分别针对个性化和高效通信两个方向，对基于联邦学习的负荷预测进行了不同形式的改进。由于个性化和通信问题这两个特点在负荷预测任务中是同时存在的，如果将两个模型简易拼装在一起，会导致模型过于复杂，其训练难度也会大大增加。因此，将两种改进方法进行有效集成是一项很有必要的工作。

（2）实际场景中存在的通信延迟问题。考虑到实际场景中不同性能的终端设备可能无法同步上传其本地模型参数，为了更贴近真实负荷预测场景，后续考虑引入异步 FL 的思想来解决该问题。

（3）新场景下的攻防策略。用户用电数据的私密性对恶意方具有吸引力，FL 的分

中国知网 https://www.cnki.net

布式特性和数据约束也为攻击者开辟了新的攻击面。因此，后续将研究相应的攻击和防御策略，以提高整个系统的鲁棒性。

中国知网 https://www.cnki.net

参 考 文 献

[1] 国家能源局. 2022 年全社会用电量同比增长 3.6%[EB/OL].[2023-1-18]. http://www.nea.gov.cn/2023-01/18/c_1310691508.htm

[2] 瞿颖. 基于差分隐私的智能电网数据收集与预测问题研究[D].南京邮电大学,2020.

[3] 李响,牛赛.双碳目标下源－网－荷多层评价体系研究[J].中国电机工程学报,2021,41(S1):178-184.

[4] 毕山松.CaO 对生物质热解过程共价键断裂影响的密度泛函理论研究[D].中国科学院大学(中国科学院工程热物理研究所),2021.

[5] 方欢欢. 智能配电网经济性评估方法研究[D].上海交通大学,2012.

[6] 王芳.电网的未来——智能电网[J].内蒙古科技与经济,2010,No.225(23):75-76+78.

[7] 蒲天骄,乔骥,韩笑,张国宾,王新迎.人工智能技术在电力设备运维检修中的研究及应用[J].高电压技术,2020,46(02):369-383.

[8] Sun L, Liu T, Xie Y, et al. Real-time power prediction approach for turbine using deep learning techniques[J]. Energy, 2021, 233: 121130.

[9] Balta-Ozkan N, Amerighi O, Boteler B. A comparison of consumer perceptions towards smart homes in the UK, Germany and Italy: reflections for policy and future research[J]. Technology Analysis & Strategic Management, 2014, 26(10): 1176-1195.

[10] 王嘉乐. 主动配电网面向用户隐私保护的终端负荷预测及分布式能源拍卖研究[D]. 东南大学,2021.

[11] Jindal A, Dua A, Kaur K, et al. Decision tree and SVM-based data analytics for theft detection in smart grid[J]. IEEE Transactions on Industrial Informatics, 2016, 12(3): 1005-1016.

[12] Chuwa M G, Wang F. A review of non-technical loss attack models and detection methods in the smart grid[J]. Electric Power Systems Research, 2021, 199: 107415.

[13] Cui L, Qu Y, Gao L, et al. Detecting false data attacks using machine learning techniques in smart grid: A survey[J]. Journal of Network and Computer Applications, 2020, 170: 102808.

[14] 程浩忠,胡枭,王莉等.区域综合能源系统规划研究综述[J].电力系统自动化,2019,43(07):2-13.

[15] 沈渊彬,刘庆珍.电力系统短期负荷预测研究概述[J].电器与能效管理技术,2016(04):28-32.

中国知网 https://www.cnki.net

[16]康重庆，夏清，刘梅．电力系统负荷预测[M]．北京：中国电力出版社，2017.

[17]周华鑫. 基于 PSOEM-LSSVM 的中长期电力负荷预测及其应用研究[D].重庆大学,2013.

[18]汪威为,陈超洋.智能电网背景下的大数据处理与短期负荷预测综述[J].无线互联科技,2019,16(05):3-5.

[19]郭松林,水泉龙,顾翔瑜.灰色系统理论在负荷预测中运用综述[J].工业仪表与自动化装置,2017(03):24-27.

[20]肖灿彬. 智能电网中基于深度学习的负荷预测研究[D].南京邮电大学,2022.

[21]詹仁俊.基于 K-means 聚类的小波支持向量机配电网短期负荷预测及应用[J].供用电,2019,36(04):64-70.

[22]孙虹,李新家,王成亮.基于需求响应的大用户电力负荷模糊综合预测研究[J].自动化与仪器仪表,2019(12):188-191.

[23]Khan G M, Khattak A R, Zafari F, et al. Electrical load forecasting using fast learning recurrent neural networks[C]//The 2013 International Joint Conference on Neural Networks (IJCNN). IEEE, 2013: 1-6.

[24]张凤林,陈峦,姚亮,鲁尔洁,杨云聪,张珺.基于信赖域法改进的BP网络在新能源并网方面的研究[J].可再生能源,2018,36(01):43-50.

[25]Shi H, Xu M, Li R. Deep learning for household load forecasting—A novel pooling deep RNN[J]. IEEE Transactions on Smart Grid, 2017, 9(5): 5271-5280.

[26]Hochreiter S, Schmidhuber J. Long short-term memory[J]. Neural computation, 1997, 9(8): 1735-1780.

[27]Kong W, Dong Z Y, Jia Y, et al. Short-term residential load forecasting based on LSTM recurrent neural network[J]. IEEE transactions on smart grid, 2017, 10(1): 841-851.

[28]Alhussein M, Aurangzeb K, Haider S I. Hybrid CNN-LSTM model for short-term individual household load forecasting[J]. Ieee Access, 2020, 8: 180544-180557.

[29]隐私保护计算与合规应用研究报告（2021 年）[EB/OL]. http://www.caict.ac.cn/kxyj/qwfb/bps/.

[30]McMahan B, Moore E, Ramage D, et al. Communication-efficient learning of deep networks from decentralized data[C]//Artificial intelligence and statistics. PMLR, 2017: 1273-1282.

[31]Abadi M, Chu A, Goodfellow I, et al. Deep learning with differential

中国知网 https://www.cnki.net

privacy[C]//Proceedings of the 2016 ACM SIGSAC conference on computer and communications security. 2016: 308-318.

[32] Mohassel P, Zhang Y. Secureml: A system for scalable privacy-preserving machine learning[C]//2017 IEEE symposium on security and privacy (SP). IEEE, 2017: 19-38.

[33] Rivest R L, Adleman L, Dertouzos M L. On data banks and privacy homomorphisms[J]. Foundations of secure computation, 1978, 4(11): 169-180.

[34] Venkataramanan V, Kaza S, Annaswamy A M. Der forecast using privacy preserving federated learning[J]. IEEE Internet of Things Journal, 2022.

[35] Qureshi N B S, Kim D H, Lee J, et al. Poisoning Attacks against Federated Learning in Load Forecasting of Smart Energy[C]//NOMS 2022-2022 IEEE/IFIP Network Operations and Management Symposium. IEEE, 2022: 1-7.

[36] Sun M, Li J, Ren Y, et al. Research on Federated Learning and Its Security Issues for Load Forecasting[C]//Proceedings of the 13th International Conference on Computer Modeling and Simulation. 2021: 237-243.

[37] Gholizadeh N, Musilek P. Federated learning with hyperparameter-based clustering for electrical load forecasting[J]. Internet of Things, 2022, 17: 100470.

[38] 袁博,葛少云,刘洪等.基于压缩感知的智能电网高级量测体系[J/OL].高电压技术:1-9[2023-03-30].

[39] Fang X, Misra S, Yang D. Smart grid. the new and improved power grid: A survey. 2012[J]. IEEE Comm. Surveys & Tutorials, 14(944-980).

[40] 刘菲菲. 基于深度学习的入侵检测算法在 AMI 中应用研究[D].兰州交通大学,2020.

[41] 郝欣宇. 移动终端下基于联合学习的车牌识别系统[D].大连理工大学,2020.

[42] Qu Y, Uddin M P, Gan C, et al. Blockchain-enabled federated learning: A survey[J]. ACM Computing Surveys, 2022, 55(4): 1-35.

[43] Şahinbaş K, Catak F O. Secure Multi-Party Computation based Privacy Preserving Data Analysis in Healthcare IoT Systems[J]. arXiv preprint arXiv:2109.14334, 2021.

[44] Zhang L, Xu J, Vijayakumar P, et al. Homomorphic encryption-based privacy-preserving federated learning in iot-enabled healthcare system[J]. IEEE Transactions on Network Science and Engineering, 2022.

[45] Jiang B, Li J, Wang H, et al. Privacy-preserving federated learning for industrial edge computing via hybrid differential privacy and adaptive compression[J]. IEEE Transactions

中国知网 https://www.cnki.net

on Industrial Informatics, 2021, 19(2): 1136-1144.

[46] Zhu H, Xu J, Liu S, et al. Federated learning on non-IID data: A survey[J]. Neurocomputing, 2021, 465: 371-390.

[47] Li D, Wang J. Fedmd: Heterogenous federated learning via model distillation[J]. arXiv preprint arXiv:1910.03581, 2019.

[48] Wang H, Kaplan Z, Niu D, et al. Optimizing federated learning on non-iid data with reinforcement learning[C]//IEEE INFOCOM 2020-IEEE Conference on Computer Communications. IEEE, 2020: 1698-1707.

[49] Arivazhagan M G, Aggarwal V, Singh A K, et al. Federated learning with personalization layers[J]. arXiv preprint arXiv:1912.00818, 2019.

[50] 李群,陈思光.基于选择性通信策略的高效联邦学习研究[J/OL].小型微型计算机系统:1-8[2023-04-06].

[51] Guha N, Talwalkar A, Smith V. One-shot federated learning[J]. arXiv preprint arXiv:1902.11175, 2019.

[52] Yao X, Huang C, Sun L. Two-stream federated learning: Reduce the communication costs[C]//2018 IEEE Visual Communications and Image Processing (VCIP). IEEE, 2018: 1-4.

[53] Luping W, Wei W, Bo L I. CMFL: Mitigating communication overhead for federated learning[C]//2019 IEEE 39th international conference on distributed computing systems (ICDCS). IEEE, 2019: 954-964.

[54] Tao Z, Li Q. eSGD: Commutation Efficient Distributed Deep Learning on the Edge[J]. HotEdge, 2018: 6.

[55] Liu L, Zhang J, Song S H, et al. Client-edge-cloud hierarchical federated learning[C]//ICC 2020-2020 IEEE International Conference on Communications (ICC). IEEE, 2020: 1-6.

[56] Konečný J, McMahan H B, Yu F X, et al. Federated learning: Strategies for improving communication efficiency[J]. arXiv preprint arXiv:1610.05492, 2016.

[57] Han S, Mao H, Dally W J. Deep compression: Compressing deep neural networks with pruning, trained quantization and huffman coding[J]. arXiv preprint arXiv:1510.00149, 2015.

[58] Huang A, Chen Y, Liu Y, et al. RPN: A residual pooling network for efficient federated learning[J]. arXiv preprint arXiv:2001.08600, 2020.

中国知网 https://www.cnki.net

[59] Shokri R, Stronati M, Song C, et al. Membership inference attacks against machine learning models[C]//2017 IEEE symposium on security and privacy (SP). IEEE, 2017: 3-18.

[60] Alistarh D, Grubic D, Li J, et al. QSGD: Communication-efficient SGD via gradient quantization and encoding[J]. Advances in neural information processing systems, 2017, 30.

[61] Mao Y, Zhao Z, Yan G, et al. Communication-efficient federated learning with adaptive quantization[J]. ACM Transactions on Intelligent Systems and Technology (TIST), 2022, 13(4): 1-26.

[62] Dwork C. Differential privacy[C]//Automata, Languages and Programming: 33rd International Colloquium, ICALP 2006, Venice, Italy, July 10-14, 2006, Proceedings, Part II 33. Springer Berlin Heidelberg, 2006: 1-12.

[63] 黄文.差分隐私机制的安全性增强及数据效用优化技术研究[D].电子科技大学,2022.

[64] Goodfellow I, Pouget-Abadie J, Mirza M, et al. Generative adversarial networks[J]. Communications of the ACM, 2020, 63(11): 139-144.

[65] 邓佳林. 基于 CNN 的滚动轴承变工况故障诊断方法研究[D].西南交通大学,2020.

[66] Jeong E, Oh S, Kim H, et al. Communication-efficient on-device machine learning: Federated distillation and augmentation under non-iid private data[J]. arXiv preprint arXiv:1811.11479, 2018.

[67] Jiang D, Shan C, Zhang Z. Federated learning algorithm based on knowledge distillation[C]//2020 International Conference on Artificial Intelligence and Computer Engineering (ICAICE). IEEE, 2020: 163-167.

[68] Sattler F, Marban A, Rischke R, et al. Communication-efficient federated distillation[J]. arXiv preprint arXiv:2012.00632, 2020.

[69] Wang T, Zhu J Y, Torralba A, et al. Dataset distillation[J]. arXiv preprint arXiv:1811.10959, 2018.

[70] Sucholutsky I, Schonlau M. Soft-label dataset distillation and text dataset distillation[C]//2021 International Joint Conference on Neural Networks (IJCNN). IEEE, 2021: 1-8.

[71] Zhao B, Mopuri K R, Bilen H. Dataset condensation with gradient matching[J]. arXiv preprint arXiv:2006.05929, 2020.

[72] Cazenavette G, Wang T, Torralba A, et al. Dataset distillation by matching training

中国知网 https://www.cnki.net

trajectories[C]//Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition. 2022: 4750-4759.

[73] Rosasco A, Carta A, Cossu A, et al. Distilled replay: Overcoming forgetting through synthetic samples[C]//Continual Semi-Supervised Learning: First International Workshop, CSSL 2021, Virtual Event, August 19–20, 2021, Revised Selected Papers. Cham: Springer International Publishing, 2022: 104-117.

[74] Zhao B, Bilen H. Dataset condensation with differentiable siamese augmentation[C]//International Conference on Machine Learning. PMLR, 2021: 12674-12685.

[75] Dong T, Zhao B, Lyu L. Privacy for free: How does dataset condensation help privacy?[C]//International Conference on Machine Learning. PMLR, 2022: 5378-5396.

[76] Li T, Hu S, Beirami A, et al. Ditto: Fair and robust federated learning through personalization[C]//International Conference on Machine Learning. PMLR, 2021: 6357-6368.

[77] Cui L, Qu Y, Xie G, et al. Security and privacy-enhanced federated learning for anomaly detection in IoT infrastructures[J]. IEEE Transactions on Industrial Informatics, 2021, 18(5): 3492-3500.

[78] Makonin S. HUE: The hourly usage of energy dataset for buildings in British Columbia[J]. Data in brief, 2019, 23.

[79] 王平飞. 基于时间序列的卷积 LSTM 电力负荷预测研究[D]. 四川大学,2021.DOI:10.27342/d.cnki.gscdu.2021.000782.

[80] 胡亚东. 基于分布式机器学习的基站网络流量预测方法研究[D].电子科技大学,2022.DOI:10.27005/d.cnki.gdzku.2022.002491.

[81] Xie Y, Wang Z, Gao D, et al. Federatedscope: A flexible federated learning platform for heterogeneity[J]. Proceedings of the VLDB Endowment, 2023, 16(5): 1059-1072.

[82] 孙铭. 基于蒸馏数据的多模型联邦学习[D].哈尔滨工业大学,2021.

[83] Wu Y, Li X, Kerschbaum F, et al. Towards robust dataset learning[J]. arXiv preprint arXiv:2211.10752, 2022.

[84] Zhu L, Liu Z, Han S. Deep leakage from gradients[J]. Advances in neural information processing systems, 2019, 32.

中国知网 https://www.cnki.net