计算机研究与发展
Journal of Computer Research and Development
DOI:10.7544/issn1000-1239.2019.20190414
56(10): 2243-2249, 2019

基于数据纵向分布的隐私保护逻辑回归

宋 蕾[1] 马春光[2] 段广晗[1] 袁 琪[3]
[1](哈尔滨工程大学计算机科学与技术学院 哈尔滨 150001)
[2](山东科技大学计算机科学与工程学院 山东青岛 266590)
[3](齐齐哈尔大学通信与电子工程学院 黑龙江齐齐哈尔 161006)
(songl@hrbeu.edu.cn)

Privacy-Preserving Logistic Regression on Vertically Partitioned Data

Song Lei[1], Ma Chunguang[2], Duan Guanghan[1], and Yuan Qi[3]
[1](*College of Computer Science and Technology, Harbin Engineering University, Harbin* 150001)
[2](*College of Computer Science and Engineering, Shandong University of Science and Technology, Qingdao, Shandong* 266590)
[3](*College of Telecommunication and Electronic Engineering, Qiqihar University, Qiqihar, Heilongjiang* 161006)

Abstract Logistic regression is the important algorithms of machine learning. Traditional training methods require centralized collection of training data which will cause privacy issues. To solve this problem, this paper proposes privacy-preserving logistic regression. This scheme is suitable for dividing data by feature dimension, and the training data is shared between two parties. The two parties conduct collaborative training and learn a shared model. In this scheme, the two parties train the model locally on private data set while exchanging the intermediate calculation results without directly exposing their private data. Additionally, the additively homomorphic scheme can ensure the calculation security which can be performed on the cipher text. During the training process, the participants can only obtain zero knowledge of each other and cannot get any information about model parameters and training data of another participant. At the same time, a privacy protection prediction method is provided to ensure that the model deployment server cannot obtain the private data of the inquirer. After analysis and experimental verification, within the tolerable loss of precision, the scheme is secure against semi-honest participants and provide privacy protection.

Key words logistic regression; privacy-preserving; homomorphic encryption; collaborative training; vertically partitioned data

摘 要 逻辑回归是机器学习的重要算法之一,为解决集中式训练方式不能保护隐私的问题,提出隐私保护的逻辑回归解决方案,该方案适用于数据以特征维度进行划分,纵向分布在两方情况下,两方进行协作式训练学习到共享的模型结构.两方在本地数据集上进行训练,通过交换中间计算结果而不直接暴露私有数据,利用加法同态加密算法在密文下进行运算保证计算安全,保证在交互中不能获取对方的敏

收稿日期:2019-06-12;**修回日期**:2019-08-05
基金项目:国家自然科学基金项目(61472097);黑龙江省自然科学基金项目(JJ2019LH1770)
This work was supported by the National Natural Science Foundation of China (61472097) and the Natural Science Foundation of Heilongjiang Province of China (JJ2019LH1770).
通信作者:马春光(machunguang@hrbeu.edu.cn)

感信息.同时,提供隐私保护的预测方法,保证模型部署服务器不能获取询问者的私有数据.经过分析与实验验证,在几乎不损失精度的前提下,该案可以在两方均是半诚实参与者情况下提供隐私保护.

关键词 逻辑回归;隐私保护;同态加密;协作训练;数据纵向分布

中图法分类号 TP391

得益于计算资源的丰富及大数据积累,近年来机器学习在视觉、自然语言处理、医疗健康等领域取得突破性进展.在机器学习技术飞速发展的同时,其安全与隐私问题也引起人们广泛关注.传统的机器学习训练方法是将训练数据收集起来进行集中训练.然而,训练数据通常会涉及到人们的隐私,如医疗健康数据、兴趣爱好、政治偏向等.将私有数据直接暴露给数据收集者进行模型训练,这种传统的模式已经不能适用于当下人们隐私保护意识增强的社会环境中.《中华人民共和国网络安全法》和欧洲《通用数据保护条例》相继颁布实施,预示对数据的安全使用和个人信息的隐私保护越发严格,给基于数据训练的机器学习方法带来前所未有的挑战.

为解决以上问题,本文提出隐私保护的逻辑回归解决方案.逻辑回归作为机器学习的典型算法,适用于分类问题.一个逻辑回归的单元可以看作为一个神经元,多个多层神经元叠加就组成了神经网络.解决逻辑回归算法的隐私保护问题是实现隐私保护机器学习的重要一步.为打破数据壁垒,如何在数据纵向分布场景中,保护隐私的情况下进行协作式、联合训练,实现逻辑回归算法是本文关注的重点.数据纵向分布,即数据以特征维度切分存储在两方,在现实中较为常见.如公司 A 和公司 B 拥有相同的用户,但业务不同.现 A 和 B 两方联合起来训练一个共同的模型,训练数据作为商业机密不能直接与对方分享.文献[1]已经实现数据纵向分布时的逻辑回归算法,利用中心服务器协助两方进行训练,客户端本地计算时使用乘法掩码.而本文实现 2 个参与方直接进行训练,并且只加密中间计算结果,利用加法掩码防止梯度信息泄露.相比之下,本文计算和通信开销更小.

本文的主要贡献有 3 个方面:

1) 在数据纵向分布的情况下,提出两方协作式的逻辑回归方案.2 个参与方在各自数据集上进行训练,通过交换中间参数,学习得到一个共同的虚拟模型.

2) 利用 Paillier 同态加密保证计算安全,保护用户隐私.通过改变逻辑回归的目标函数,使其适用于加法同态加密方案来实现两方密文计算,保证交互及运算过程中安全性,不泄露用户隐私信息.

3) 本文给出隐私保护的预测方案,实现用户秘密预测.用户不暴露自身数据,而服务器也不能知晓用户的预测结果.

1 相关工作

2015 年 Shokri 和 Shmatikov[2] 提出协作式隐私保护深度学习模型,每轮训练各方参与者从中心服务器下载最新模型参数,利用私有数据在本地训练模型,再上传更新服务模型.无需集中存储训练数据,从而保护用户敏感的训练数据;2018 年 Phong 等人[3]利用加法同态加密算法加密模型参数,防止泄露梯度信息给诚实且好奇的中心服务器;2016 年由 Google[4]提出联邦学习用于预测 Android 手机键盘下一个输入词;类似于文献[2]用户在手机上训练模型再将参数上传到服务端,不同的是,为保证模型参数的安全聚合,使用秘密共享及安全多方计算协议保障用户隐私信息[5-6];2019 年 Yang 等人[7]给出联邦学习正式定义,指数据拥有方在不暴露自身数据的前提下进行模型训练得到虚拟共有模型的过程,其模型与将各方数据聚集在一起训练所得到的模型差距足够小.同时根据数据分布,将联邦学习分为横向联邦学习、纵向联邦学习和联邦迁移学习;Hardy 等人[1]实现纵向联邦学习逻辑回归算法,利用加法同态加密算法保障计算安全;SecureML[8]利用秘密共享、姚式电路,实现了一种有效保护隐私的,用于线性回归、逻辑回归和神经网络训练两方安全计算协议;Mohassel 等人[9]将该方案扩展到三方安全计算;Ma 等人[10]对文献[8]进行改进,实现非交互式隐私保护神经网络预测;DeepSecure[11]利用姚式电路实现两方安全计算,完成深度学习模型的安全预测.

不同于以上工作,本文关注于数据纵向分布的情况下,提出隐私保护的逻辑回归训练方法和预测方法.

2　基本定义及预备知识

本节主要介绍本文要解决的问题及其安全性定义.在2.3节介绍同态加密算法.

2.1　问题定义

逻辑回归是标准的有监督机器学习算法,设有训练数据集$\{\boldsymbol{x}_i,y_i\}_{i=1}^N$,其中$\boldsymbol{x}_i=(x_{i1},x_{i2},\cdots,x_{id})$,$\boldsymbol{x}\in\mathbb{R}^d$是$d$维特征向量,$y\in\{0,1\}$.将学习到模型$f$的一组参数$\boldsymbol{\theta}\in\mathbb{R}^{d+1}$,使得样本$\boldsymbol{x}_i$映射到$\{0,1\}$的标签中.

在数据纵向分布在2个客户端A,B时,设A有训练数据$\{\boldsymbol{x}_i^A\}_{i=1}^N$,其中$\boldsymbol{x}_i^A=(x_{i1},x_{i2},\cdots,x_{ij})$,$B$有训练数据及其标签$\{\boldsymbol{x}_i^B,y_i\}_{i=1}^N$,其中$\boldsymbol{x}_i^B=(x_{i(j+1)},x_{i(j+2)},\cdots,x_{id})$,$1<j<d$.$A$和$B$通过联合、协作的方式训练一个逻辑回归模型,在训练过程中A和B的训练数据均在本地,不能泄露任何有关训练数据的信息.

2.2　安全性定义

假设A和B是非共谋、半诚实的参与者.A和B在协作期间遵守模型训练协议,但互相对对方的私有数据及模型参数是好奇的,在协作期间不断推理,想要获取关于对方额外的信息.如果在训练过程中,A和B不能获得对方额外的敏感信息,如训练数据及模型参数,则称训练过程是安全的.如果在预测阶段,模型部署在A和B上,询问者在预测过程中,A和B不能获得询问者的私有数据,则称预测过程是安全的.

2.3　同态加密

同态加密(HE)[12]可以实现在不知道密钥的情况下对加密数据进行安全计算,其运算结果解密后与直接在明文上计算结果相同.一个同态加密方案主要包含:秘钥生成、加密算法、解密算法.全同态加密(FHE)可以执行加法和乘法运算.但是全同态加密方案计算开销大,本文两方计算只涉及到加法操作,因此本文选用快速的加法同态加密方案Paillier,Paillier[13]加密方案工作原理为:

秘钥生成$(pk,sk)\leftarrow keyGen(\cdot)$随机选择2个长度相等的大质数$p$和$q$,计算$n=pq$,$\varphi(n)=(p-1)(q-1)$,选择随机数$g$满足$g\in\mathbb{Z}_{n^2}^*$,则公钥$pk=(n,g)$,私钥$sk=(\varphi(n),\varphi(n)^{-1}\bmod n)$.

加密算法$c\leftarrow E(pk,m)$.给明文m,选择一个随机数r,满足$0<r<n$且$r\in\mathbb{Z}_{n^2}^*$,输出密文$c=g^m\times r^n \bmod n^2$.

解密算法$m\leftarrow D(sk,c)$.给密文c,输出明文$m=L(c^{\varphi(n)}\bmod n^2)\times\varphi(n)^{-1}\bmod n$,其中$L(x)=\dfrac{(x-1)}{n}$.

3　隐私保护逻辑回归

在本节中,我们主要介绍隐私保护逻辑回归算法,其具体包括密文梯度计算过程、隐私保护下的训练过程及隐私保护下的预测过程.

3.1　密文梯度计算过程

逻辑回归将线性模型的产生的预测值通过激活函数$g(\boldsymbol{\theta x})=\dfrac{1}{1+\mathrm{e}^{-\boldsymbol{\theta x}}}$映射到0～1之间,$g(z)\geqslant 0.5$时标签为1,$g(z)<0.5$时标签为0.其目标函数为

$$L(\boldsymbol{\theta})=\sum_{i=1}^{N}-y_i\boldsymbol{\theta x}_i+\ln(1+\mathrm{e}^{\boldsymbol{\theta x}_i}),\tag{1}$$

通过最小化目标函数即可得到模型参数$\boldsymbol{\theta}$.

在两方协作训练中,设$\boldsymbol{\theta}^A$,$\boldsymbol{\theta}^B$是A和B的模型参数,令$u_i^A=\boldsymbol{\theta}^A\boldsymbol{x}_i^A$,$u_i^B=\boldsymbol{\theta}^B\boldsymbol{x}_i^B$,则联合目标函数为

$$L=\sum_{i=1}^{N}-y_i(u_i^A+u_i^B)+\ln(1+\mathrm{e}^{u_i^A+u_i^B}),\tag{2}$$

则模型A和B参数更新为

$$\begin{aligned}\boldsymbol{\theta}^A&:=\boldsymbol{\theta}^A-\eta\frac{\partial L}{\partial\boldsymbol{\theta}^A},\\ \boldsymbol{\theta}^B&:=\boldsymbol{\theta}^B-\eta\frac{\partial L}{\partial\boldsymbol{\theta}^B}.\end{aligned}\tag{3}$$

为达到隐私保护的目的,使用同态加密算法加密u_i^A和u_i^B确保计算安全.由于同态加密只能计算多项式函数,故使用泰勒公式在0点展开,近似模拟目标函数.因为有:

$$\ln(1+\mathrm{e}^z)\approx\ln 2+\frac{1}{2}z+\frac{1}{8}z^2+O(z^4),\tag{4}$$

则式(2)转换为

$$\begin{aligned}L\approx\sum_{i=1}^{N}&-y_i(u_i^A+u_i^B)+\frac{1}{2}(u_i^A+u_i^B)+\\&\frac{1}{8}(u_i^A+u_i^B)^2+\ln 2.\end{aligned}\tag{5}$$

因为$\ln 2$为常数,在最小化L的过程中并不影响结果,因此以下公式中将省略$\ln 2$.设$[\cdot]$为A和B使用同态加密后的结果.则加密后的目标函数为

$$\begin{aligned}[L]=\sum_{i=1}^{N}&-y_i([u_i^A]+[u_i^B])+\frac{1}{2}([u_i^A]+\\&[u_i^B])+\frac{1}{8}[(u_i^A)^2]+\frac{1}{8}[(u_i^B)^2]+\\&\frac{1}{4}[u_i^A\times u_i^B].\end{aligned}\tag{6}$$

因为有$\frac{\partial u_i^A}{\partial \boldsymbol{\theta}^A}=\boldsymbol{x}_i^A$,$\frac{\partial u_i^B}{\partial \boldsymbol{\theta}^B}=\boldsymbol{x}_i^B$,则可到加密的梯度为

$$\left[\frac{\partial L}{\partial \boldsymbol{\theta}^A}\right]=\sum_{i=1}^{N}-[y_i]\boldsymbol{x}_i^A+\frac{1}{2}[\boldsymbol{x}_i^A]+\frac{1}{4}[u_i^A\boldsymbol{x}_i^A]+\frac{1}{4}[u_i^B]\boldsymbol{x}_i^A, \tag{7}$$

$$\left[\frac{\partial L}{\partial \boldsymbol{\theta}^B}\right]=\sum_{i=1}^{N}-[y_i\boldsymbol{x}_i^B]+\frac{1}{2}[\boldsymbol{x}_i^B]+\frac{1}{4}[u_i^B\boldsymbol{x}_i^B]+\frac{1}{4}[u_i^A]\boldsymbol{x}_i^B. \tag{8}$$

3.2 隐私保护下的训练过程

隐私保护的逻辑回归具体训练过程为:

Step1. A 和 B 分别产生一对公私钥,将公钥发给对方.

Step2. A 计算 $u_i^A=\boldsymbol{\theta}^A\boldsymbol{x}_i^A$,$(u_i^A)^2$,用公钥加密后,将$[u_i^A]_A$,$[(u_i^A)^2]_A$ 发送给 B.

Step3. B 计算 $u_i^B=\boldsymbol{\theta}^B\boldsymbol{x}_i^B$,接收到$[u_i^A]_A$,$[(u_i^A)^2]_A$ 后,根据式(6)计算得到$[L]_A$,根据式(8)计算梯度为$\left[\frac{\partial L}{\partial \boldsymbol{\theta}^B}\right]_A$,选择随机掩码 R^B,计算得到$\left[\frac{\partial L}{\partial \boldsymbol{\theta}^B}+R^B\right]_A$,将 $[L]_A$,$\left[\frac{\partial L}{\partial \boldsymbol{\theta}^B}+R^B\right]_A$,$[u_i^B]_B$,$[y_i]_B$ 发送给 A.

Step4. A 解密得到 L,$\frac{\partial L}{\partial \boldsymbol{\theta}^B}+R^B$,并根据式(7)计算梯度得到$\left[\frac{\partial L}{\partial \boldsymbol{\theta}^A}\right]_B$,选择选择随机掩码 R^A,计算得到$\left[\frac{\partial L}{\partial \boldsymbol{\theta}^A}+R^A\right]_B$,将$\frac{\partial L}{\partial \boldsymbol{\theta}^B}+R^B$,$\left[\frac{\partial L}{\partial \boldsymbol{\theta}^A}+R^A\right]_B$ 发送给 B.

Step5. B 解密得到$\frac{\partial L}{\partial \boldsymbol{\theta}^A}+R^A$,将其发送给 A.

Step6. B 得到$\frac{\partial L}{\partial \boldsymbol{\theta}^B}$,更新本地参数.

Step7. A 得到$\frac{\partial L}{\partial \boldsymbol{\theta}^A}$,更新本地参数.

重复 Step1~Step7,直到模型收敛.

3.3 隐私保护下的预测过程

当 A,B 一方作为询问者使用模型进行预测时,设询问者为 $K\in\{A,B\}$,当 $K=A$ 时,令 $K'=B$,反之亦然.

① K 将预测数据分为 $\boldsymbol{x}^K$ 和 $\boldsymbol{x}^{K'}$ 两部分,用 K 的公钥加密后$[\boldsymbol{x}^{K'}]_K$,发送给 K'.

② K 计算 $u^K=\boldsymbol{\theta}^K\boldsymbol{x}^K$.

③ K'计算$[u^{K'}]_K=\boldsymbol{\theta}^{K'}[\boldsymbol{x}^{K'}]_K$,将$[u^{K'}]_K$ 发送给 K.

④ K 用私钥解密得到 $u^{K'}$,相加得到 $u=u^K+u^{K'}$.

⑤ 最后得到最终输出结果$\frac{1}{1+\mathrm{e}^{-u}}$.

当询问者为第三方 C 时,模型部署在 A 和 B 中,预测过程和上述类似.

① C 将预测数据分为 $\boldsymbol{x}^A$ 和 $\boldsymbol{x}^B$ 两部分,用 C 的公钥加密 $\boldsymbol{x}^A$ 和 $\boldsymbol{x}^B$,得到$[\boldsymbol{x}^A]_C$ 和$[\boldsymbol{x}^B]_C$,分别发送给 A 和 B 进行计算.

② A 和 B 分别计算得到$[u^A]_C=\boldsymbol{\theta}^A[\boldsymbol{x}^A]_C$ 和$[u^B]_C=\boldsymbol{\theta}^B[\boldsymbol{x}^B]_C$,并发送给 C.

③ C 解密后得到 u^A 和 u^B,$u=u^A+u^B$,最后得到最终输出结果$\frac{1}{1+\mathrm{e}^{-u}}$.

4 隐私保护逻辑回归算法分析

4.1 安全性分析

回顾 A 和 B 的协作训练过程,得到模型后 C 进行预测的过程.在此过程中各方参与者获得的中间计算结果如表 1 所示:

Table 1 Information Obtained by Participants During the Training Process and Prediction Process

表 1 训练及预测过程中参与者获得的信息

Process	A	B	C
Training Process	$[u_i^B]_B$,$[y_i]_B$ $\frac{\partial L}{\partial \boldsymbol{\theta}^B}+R^B$,$L$	$[u_i^A]_A$,$[(u_i^A)^2]_A$ $\frac{\partial L}{\partial \boldsymbol{\theta}^A}+R^A$	
Prediction Process	$[\boldsymbol{x}^A]_C$,$[u^A]_C$	$[\boldsymbol{x}^B]_C$,$[u^B]_C$	Prediction Results

从表 1 可见,在训练过程中 A 获得$[u_i^B]_B$,$[y_i]_B$,均是用 B 的公钥加密的密文,因为 A 没有 B 的私钥因此无法获得关于 B 的任何信息.同时,A 获得$\frac{\partial L}{\partial \boldsymbol{\theta}^B}+R^B$ 是加了掩码信息后的 B 的模型参数梯度,并不能从梯度推理出更多关于 B 的信息.同理,B 也不能获得关于 A 的训练数据及模型信息.A 和 B 均在计算关于对方中间结果时均在密文下进行运算.由此可知,训练过程是安全的.

在预测阶段,A 和 B 获得的均是关于 C 的预测数据的密文$[\boldsymbol{x}^A]_C$,$[\boldsymbol{x}^B]_C$,并且均在密文下进行运算获得$[u^A]_C$,$[u^B]_C$.因此 A 和 B 无法获得关于 C 的私有数据的任何信息,预测过程是安全的.

在传输过程中,A 和 B 传输的是中间计算结果的密文,敌手即使截获信道消息也无法解密.A 和 B

之间传输的明文是加上掩码的模型参数梯度,由于敌手不知道掩码,故无法获得关于梯度的信息.因此敌手为第三方时,也无法通过信道获取任何敏感信息.

4.2　算法性能分析

与非隐私保护的逻辑回归算法相比,本文算法产生的额外开销主要包括时间开销与通信开销.时间开销主要来自于密文计算,本文使用 Paillier 加法同态加密算法,秘钥长度为 1 024 b.在 CPU 为 Intel Core i5-6500,3.20 GHz 的计算机上进行加密计算,执行时间为:

加密时间 T_E.执行 100 次耗时 1.598 s.

解密时间 T_D.执行 100 次耗时 0.507 s.

加法时间 T_A.执行 2 000 次 2 个密文相加运算耗时 0.086 s.

乘法时间 T_M.执行明文与密文之间的乘法时间与明文大小成正比.在本文算法训练过程中,只需执行 1/2,1/4,1/8 乘以密文,执行 2 000 次耗时平均为 1.364 s.

分析忽略通信过程中的传送时间,训练过程中选取 $batch\_size$ 大小为 n,在一个迭代周期内,加密时间复杂度为 $O(n\times T\_E)$,解密时间复杂度为 $O(n\times T\_D)$.计算[L]时间复杂度为 $O(n\times T\_M)$,计算 A 方梯度的时间复杂度为 $O(n\times d_A\times T\_M)$,计算 B 方梯度的时间复杂度为 $O(n\times d_B\times T\_M)$,其中 d_A,d_B 分别为 A 和 B 数据的特征维数.

在训练过程中,A 和 B 之间的通信开销为 $Cost=2(3\times n\times ct+ct)$,其中 ct 为一条密文大小.空间复杂度为 $O(n\times ct)$.在 $batch\_size=64$,$ct=256$ b,一个迭代过程中通信开销约为 12 KB.

5　实验与结果

在本节中,我们搭建了本文提出的基于数据纵向分布的隐私保护逻辑回归模型,并且在 7 组数据集上测试了本文方案.

5.1　数据集描述

本文在 4 组随机生成的 2 分类数据集与 3 组现有的分类数据集上对所提出的模型进行测试,下面从数据维度、数据大小等方面对数据集进行介绍.

MC-1 数据集与 MC-2 数据集是使用 Python 的机器学习模块 scikit-learn 提供的 make_classification 函数构建的用于训练分类模型的数据集,其中 MC-1 数据集包含 2 000 条特征维度为 6 的数据,这些数据属于 2 个分类.MC-2 是包含 2 000 条特征维度为 10 的 2 分类数据.MB-1 数据集与 MB-2 数据集是使用 scikit-learn 提供的 make_blobs 函数生成的用于聚类的数据集,其中 MB-1 数据集包含 1 000 条特征维度为 6、方差为 5 的具有 2 个聚类中心点的数据,MB-2 数据集包含 1 000 条特征维度为 10、方差为 6 的具有 2 个聚类中心点的数据.

digits 是手写数字数据集,该数据集包含了 1 797 个共计 10 个分类的手写数字数据,其原始数据尺寸为 8×8 像素,其中每个像素点用整数 0～16 来表示其灰阶.为验证本文提出的基于数据纵向分布的隐私保护逻辑回归模型,我们将数字 0～4 设定为分类 1,将数字 5～9 设定为分类 2,将多分类问题简化为 2 分类问题.同时我们从 digits 数据集中抽取出数字 7 与 9 组成一个 2 分类数据集(digits-79),用以验证样本量较小时本文提出的模型性能.breastcancer 是一个包含 2 分类数据的乳腺癌数据集,其中包含了 569 组特征维度为 30 样本.

对上述的全部数据集,我们将其特征均等纵分为 2 部分分别交给 A,B 双方,我们随机抽取其中的 70%样本用于训练模型,剩余的 30%样本用于测试模型性能.

5.2　实验和结果分析

在本节中,进行 7 组实验来验证本文提出模型的有效性.在所有的实验中,我们采用学习率为 0.01 的随机梯度下降法对模型进行训练,同时对于所有输入的数据,对其进行归一化处理以易于模型收敛到最优解.

使用泰勒展开式模拟原有的目标函数,会对训练过程收敛速度及精度产生一定影响.本文通过实验从 3 方面对具体差异进行评估,首先对比原目标函数和用泰勒公式近似的目标函数 2 个模型在训练过程中的 $Loss$ 变化曲线,如图 1 所示.采用泰勒公式近似的目标函数的逻辑回归模型,其 $Loss$ 的收敛速度与采用原目标函数的逻辑回归模型差别不大.其次,对原目标函数和用泰勒公式近似的目标函数 2 个模型的训练精度进行了实验,如图 2 所示.在经过 200 次迭代后,采用泰勒公式近似的目标函数模型的预测精度趋近于稳定,此时其预测精度高于采用原目标函数的逻辑回归模型;在 400 次迭代后,采用原目标函数的逻辑回归模型预测精度与采用泰勒公式近似的目标函数模型几乎相同,随着训练的继续进行;在 800 次迭代后,采用原目标函数的逻辑回归模型预测精度达到稳定状态,原模型的最终预测精度略高于采用泰勒公式近似的目标函数模型.

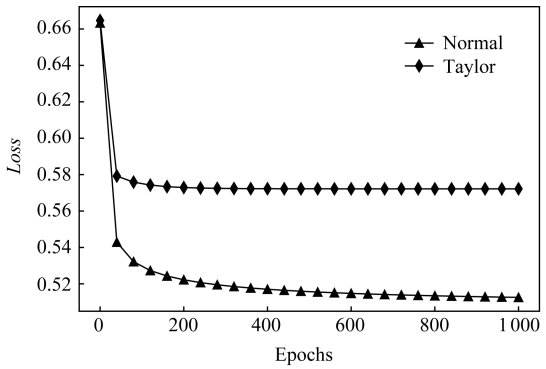

Fig. 1 Comparison of *Loss* during training process

图 1 训练过程 *Loss* 变化曲线对比图

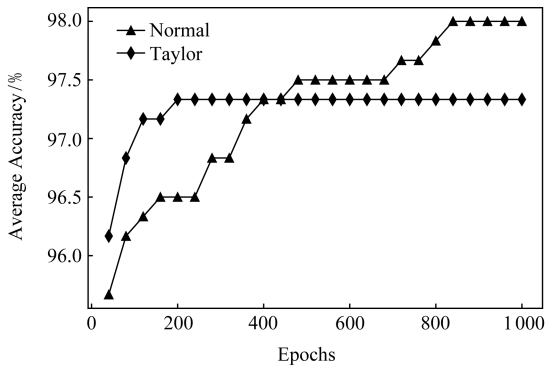

Fig. 2 Comparison of performance between two models

图 2 2 种模型测试精度对比图

本文在 7 组数据集上对 2 种模型进行分类实验,表 2 给出了 2 种模型的分类精度与 *AUC*(area under curve).其中,*AUC* 是 ROC 曲线下与横坐标轴围成的面积,其值通常在 0.5～1 之间,*AUC* 的值越大,说明分类器的分类效果越好.从表 2 可以看出,采用原目标函数的逻辑回归模型与采用泰勒公式近似目标函数的逻辑回归模型在 7 组数据集上的预测精度与 *AUC* 差别不大,这说明本文提出的基于数据纵向分布的隐私保护逻辑回归在预测精度和模型性能没有明显损失的前提下,保护了训练数据的隐私.

Table 2 Results on Two Models

表 2 在 2 种模型上的分类精度实验结果

Dataset	Sample Size	Feature Dimention	Logistic		Taylor	
			Accuracy/%	*AUC*	*Accuracy*/%	*AUC*
MC-1	2 000	6	98.33	0.992 7	97.67	0.993 4
MC-2	2 000	10	98.00	0.990 6	97.33	0.990 4
MB-1	1 000	6	94.67	0.991 5	93.67	0.990 8
MB-2	1 000	10	98.00	0.997 1	98.67	0.997 8
breastcancer	569	30	81.29	0.964 1	81.87	0.964 1
digits	1 797	64	89.44	0.954 2	89.63	0.956 6
digits-79	359	64	97.22	0.997 9	97.22	0.997 9

6 总 结

本文提出了在数据纵向分布下的隐私保护逻辑回归解决方案,不仅实现隐私保护的训练过程,同时给出隐私保护的预测过程.保证在训练过程中,协作的双方不能获得对方的训练数据及其模型参数信息.在预测过程中,保护访问者的私有数据不泄露给部署模型的服务器.根据分析及实验得出,本文方案可以在可容忍的精度损失下提供隐私保护需求.训练数据纵向分布,双方协作共同训练模型在现实中具有广泛的应用价值.未来将会把本文中隐私保护逻辑回归扩展到深度学习中,并且寻求高效的加密算法降低计算开销.

参 考 文 献

[1] Hardy S, Henecka W, Ivey-Law H, et al. Private federated learning on vertically partitioned data via entity resolution and additively homomorphic encryption [J]. arXiv preprint arXiv:1711.10677, 2017

[2] Shokri R, Shmatikov V. Privacy-preserving deep learning [C] //Proc of the 22nd ACM SIGSAC Conf on Computer and Communications Security. New York: ACM, 2015: 1310-1321

[3] Phong L T, Aono Y, Hayashi T, et al. Privacy-preserving deep learning via additively homomorphic encryption [J]. IEEE Transactions on Information Forensics and Security, 2018, 13(5): 1333-1345

[4] McMahan H B, Moore E, Ramage D, et al. Communication efficient learning of deep networks from decentralized data [J]. arXiv preprint arXiv:1602.05629, 2016

[5] Bonawitz K, Ivanov V, Kreuter B, et al. Practical secure aggregation for privacy-preserving machine learning [C] // Proc of the 2017 ACM SIGSAC Conf on Computer and Communications Security. New York: ACM, 2017: 1175-1191

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

[7] Yang Qiang, Liu Yang, Chen Tianjian, et al. Federated machine learning: Concept and applications [J]. ACM Transactions on Intelligent Systems and Technology, 2019, 10(2): 1-19

[8] Mohassel P, Zhang Yupen. SecureML: A system for scalable privacypreserving machine learning [C] //Proc of 2017 IEEE Symp on Security and Privacy (SP). Piscataway, NJ: IEEE, 2017: 19-38

[9] Mohassel P, Rindal P. ABY 3: A mixed protocol framework for machine learning [C] //Proc of the 2018 ACM SIGSAC Conf on Computer and Communications Security. New York: ACM, 2018: 35-52

[10] Ma Xu, Chen Xiaofeng, Zhang Xiaoyu, et al. Non-interactive privacy-preserving neural network prediction [J]. Information Sciences, 2019, 481: 507-519

[11] Rouhani B D, Riazi M S, Koushanfar F. DeepSecure: Scalable provably-secure deep learning [C] //Proc of the 55th Annual Design Automation Conf. New York: ACM, 2018: 2:1-2:6

[12] Brakerski Z, Gentry C, Vaikuntanathan V. (Leveled) fully homomorphic encryption without bootstrapping [J]. ACM Transactions on Computation Theory, 2014, 6(3): 13:1-13:36

[13] Paillier P. Public-key cryptosystems based on composite degree residuosity classes [C] //Proc of the 18th Int Conf on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 1999: 223-238

Song Lei, born in 1989. PhD candidate. Her main research interests include machine learning, artificial intelligence and security, federated learning.

Ma Chunguang, born in 1974. PhD, professor, PhD supervisor. His main research interests include post-quantum cryptography, distributed cryptographic protocol, cloud computing security and privacy, artificial intelligence and security, block chain technology and application, etc.

Duan Guanghan, born in 1994. PhD candidate. His main research interests include machine learning, artificial intelligence and security, adversarial examples.

Yuan Qi, born in 1973. PhD, associate professor. Her main research interests include block chain, artificial intelligence and information security.