Mathematical Biosciences and Engineering

http://www.aimspress.com/journal/MBE

MBE, 18(4): 4772–4796.
DOI: 10.3934/mbe.2021243
Received: 09 April 2021
Accepted: 18 May 2021
Published: 01 June 2021

Research article

Guaranteed distributed machine learning: Privacy-preserving empirical risk minimization

Kwabena Owusu-Agyemang, Zhen Qin*, Appiah Benjamin, Hu Xiong and Zhiguang Qin

University of Electronic Science and Technology of China, School of Information and Software Engineering, China

* **Correspondence:** Email: qinzhen@uestc.edu.cn.

Abstract: Distributed learning over data from sensor-based networks has been adopted to collaboratively train models on these sensitive data without privacy leakages. We present a distributed learning framework that involves the integration of secure multi-party computation and differential privacy. In our differential privacy method, we explore the potential of output perturbation and gradient perturbation and also progress with the cutting-edge methods of both techniques in the distributed learning domain. In our proposed multi-scheme output perturbation algorithm (MS-OP), data owners combine their local classifiers within a secure multi-party computation and later inject an appreciable amount of statistical noise into the model before they are revealed. In our Adaptive Iterative gradient perturbation (MS-GP) method, data providers collaboratively train a global model. During each iteration, the data owners aggregate their locally trained models within the secure multi-party domain. Since the conversion of differentially private algorithms are often naive, we improve on the method by a meticulous calibration of the privacy budget for each iteration. As the parameters of the model approach the optimal values, gradients are decreased and therefore require accurate measurement. We, therefore, add a fundamental line-search capability to enable our MS-GP algorithm to decide exactly when a more accurate measurement of the gradient is indispensable. Validation of our models on three (3) real-world datasets shows that our algorithm possesses a sustainable competitive advantage over the existing cutting-edge privacy-preserving requirements in the distributed setting.

Keywords: Internet of Things; differential privacy; fully homomorphic encryption; privacy-preserving; secure multi-party computations; human activity recognition

1. Introduction

With the proliferation of Mobile Sensor Networks [1], mobile devices (i.e., smartphones, tablets, personal digital assistant, laptop computers, smart watches, e-readers) are widely preferred by users since it is gradually occupying an imperative position in sensor-based activity recognition [2], coupled with the rapid growth of its per capita holding. Privacy-preserving [3] is a fundamental challenge for the massive structured and unstructured [4] datasets generated in these numerous smart applications that rely on data aggregation and combined learning across diverse nodes. Existing approaches take different methods to address these privacy concerns. Two predominant approaches are secure Multiparty Computation (MPC) and Differential Privacy (DP) [5].

MPC is a preferred option to optimize a computational function over jointly distributed data resources with the application of cryptographic primitives (i.e., oblivious transfer, secret sharing, and homomorphic encryption) whiles keeping these data private. MPC under different adversarial models have been studied in numerous computer domains (e.g., [6]). One of the initial private data mining methods in this domain was proposed by Lui et al. [7], which was preceded by plethora of works considering various applications or implementation of adversarial models. Most of the existing MPC primitives to help meet the secure requirements are based on the advancement in fully homomorphic encryption (FHE) [8]. It enables data providers to encrypt individual datasets with the public key and outsource a computation to the cloud server. The cloud server computes on the encrypted datasets and therefore generates encrypted intermediate results. In the absence of the secrete key, cloud server basically serves as a computation platform that is unable to access any of the individual records. Current emphasis has been on achieving realistic and efficient Distributed machine learning (DML)with the application of MPC primitives [9], and in some domains these approaches have demonstrated to scale hundreds of millions of records to learning tasks [10]. Notwithstanding the considerable benefits of MPC, it still has an inevitable obstacle: issues of security and privacy. The cloud server may be semi-honest and even malicious in specific cases, which means it may be motivated to infer from the individual's confidential information for profit or curiosity during the training of the machine learning models. This is becoming a non-trivial privacy concern for outsourced secure multiparty computation.

Differential privacy comes in handy to inject noise into the intermediate results to avoid inferring sensitive information about any specific individual record. However, in order to balance privacy and model usability, careful calibration of the statistical noise is required. Conversely, accomplishing the trade-off amid the privacy and utility of the DP algorithm still remains a problem. Concretely, unlike prevailing approaches involving the use of differential privacy on classifiers, they only protect the training data during the learning process; there is no focus on mitigating the privacy risk of black-box inference attacks on the resultant machine learning model. In the architecture of differential privacy, Empirical Risk Minimization (ERM) plays a crucial role as it encompasses a myriad of tasks in machine learning. In cases where one knows how to implement ERM privately (DP-ERM), for extended machine learning problems, essentially regression and classification, it, therefore, becomes easy to obtain differentially private algorithms. The initial representative works in this line of study was conducted by [11]. DP-ERM should have indistinguishable intermediate results when there is a small modification in the input datasets. Specifically, earlier studies on DP-ERM to guarantee differentially private optimization are based on three methods: Objective Perturbation, Output Perturbation (OP), and Gradient Perturbation(GP).

Concretely, existing approaches have demonstrated that it may be applied to permit privacy-preserving in the centralized domain with an individual entity possessing the entire dataset. However, there is a more prevailing problem where data is owned by multiple organizations in the distributed domain. Consider the real-world application of this paradigm in medical research where multiple hospitals may wish to collaboratively train a model with the application of the sensor-based activities recognition medical records generated from a large number of patient wearable mobile devices without exposing their individual data instances to other parties. This powerful method has been integrated with Distributed machine learning in the pioneering study of Pathak et al. [12] , which securely aggregates locally trained classifiers with the application of output perturbation to establish differential privacy. Since the allocated noise in the model is inversely proportional to the smallest dataset with p parties, Jayaraman et al. [13] later improved the noise scale by a factor of $\sqrt{p}$ with the adoption of secure model aggregation of locally trained classifiers [14] and then execute naïve aggregation of the locally trained models whiles providing meaningful privacy guarantee. Their proposed output perturbation algorithm is capable of improving Pathak et al.'s [12] protocol by a component of p by injection of statistical noise within the secure MPC domain based on a required noise scale which is inversely proportional to the volume of the whole dataset.

Despite the recurrent progress in such markets, for several hospitals to deploy mobile sensor networks in a Pervasive healthcare monitoring setup to accumulate health dataset through mobile devices to develop innovative diagnostic classifiers from these patient records, there are still quite some few threatening issues:

(a) Such existing works [12, 13] provides model parameters without any uncertainty. Therefore, making it extremely difficult to add capabilities for quantifying uncertainty in the model coefficients.

(b) In cases where the data is extremely huge with each individual data provider having only one training instance, application of classifier aggregation method for generating a global model from multiple locally trained classifiers based on the use of parameter averaging technique may lead to information leakages. Since the parameter averaging is only applicable to the collection of the same model type, which will also tend to generate less accurate global aggregated classifiers in comparison to the centralized domain.

(c) Since the accuracy of the model relies heavily on the pre-specified amount of iterations -*T*, in situations where the iteration is too little, the learning procedure will discontinue well short of the optimal, and the larger the iteration, the smaller the privacy budget ϵ_t for each iteration. therefore, it requires large volumes of statistical noise to be injected at every gradient iteration, hence causing the swamping of the signal contributed by the gradient in the iterative training procedure.

(d) In the initial stage of ERM optimization, gradients are anticipated to remain very huge, this is to enable the learning algorithm to find adequate parameter updates irrespective of when the gradient is not computed accurately. Nonetheless, the gradient begins to decrease and requires accurate measurement as the current parameter w_t approaches the optimal values. This is to enable the optimization algorithm to continue minimizing or approximately minimizing the loss function f. This implies that on the grounds that total privacy cost remains unchanged it is important to apply an adaptive iterative privacy budget allotment than a fixed allotment.

The basic pipeline for securely training distributed machine learning models in this scenario is illustrated in Figure 1, where the secure multi-party machine learning framework is a composition of p + *1* data providers $\{\emptyset_1, \emptyset_2, \ldots, \emptyset_p\}$ and a cloud server. In this architecture , the assumption is that each data provider $\emptyset_i$, who holds their individual private dataset $\mathcal{D}_i$ medical records and a training model θ generated from the dataset, is willing to improve the accuracy of the globally trained model without leaking any sensitive information about the locally owned confidential dataset.

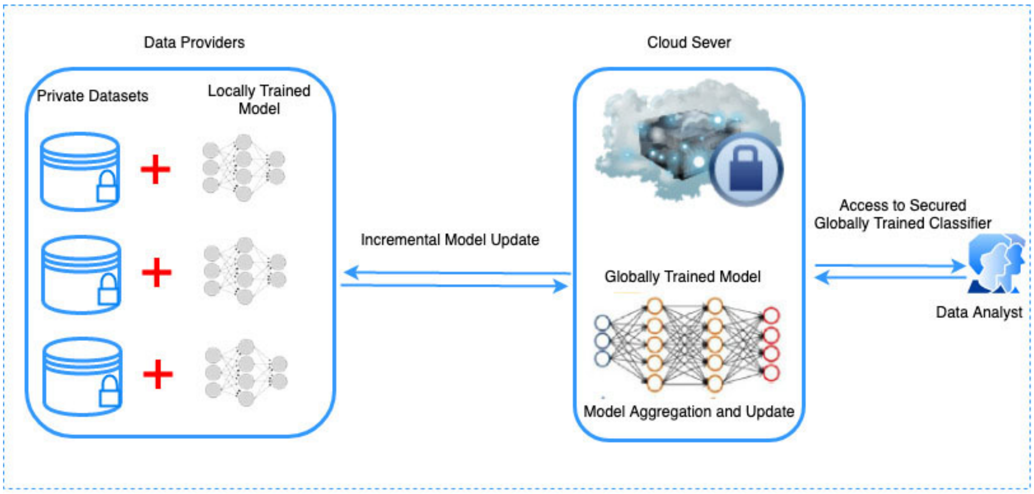

Figure 1. Secure distributed machine learning and description pipeline.

In this paper, we argue that it is of great significance to introduce differentially-private distributed machine learning algorithms to thrash out the three outlined fundamental problems in the current protocol [13, 14]. We apply both output perturbation and gradient perturbation with the injection of statistical noise inside a secure multi-party computation domain. The inherent strategy is to demonstrate that our output perturbation algorithm securely aggregates the locally trained models which are encrypted with distinct encryption primitives or even with distinctive keys to achieving ϵ-differential privacy with the addition of statistical Laplace noise to the aggregated classifiers parameters. In our gradient perturbation scheme, individual data owners jointly execute an adaptive iterative gradient-based protocol where they securely aggregate the local gradients per each iteration with distinctive share ϵ_t of the total privacy budget ϵ. Therefore providing (ϵ,δ)-differential privacy with the application of adaptive gradient descent approach for zero-mean Concentrated DP [15] (zCDP).

This protocol offers (ϵ, δ)-differential privacy guarantee in the honest-but-curious security threat environment by the underlying cryptosystem and privacy-preserving primitives. In this domain, adversaries may only obtain negligible opportunities to leak the sensitive data instance since the individual models are globally encrypted. It provides a more practicable and efficiency privacy-preserving primitive in the Distributed machine learning domain.

The principal contribution to this work can be summarized in threefold:

- To strongly achieve computationally more efficient and also maintain higher accuracy irrespective of how the dataset is partitioned when accurate machine learning models are privately trained in the distributed setting, we apply noise bounds for each of our two chosen protocols; multi-scheme output perturbation (MS-OP) and gradient perturbation (MS-GP) method in our proposed algorithm.

- For our gradient perturbation method, we present a private gradient descent protocol based on zCDP [15] which is more robust than (ϵ, δ)-differential and also attain minimum known bound on the privacy budget. In this algorithm step size per iteration and privacy, the budget is dynamically decided at run-time grounded on the value of injected statistical noise obtained for the current iteration of the gradient. Additionally, the noise is generated within the secure multiparty protocol. This will enable us to inject a unique copy of statistical noise as compared to existing approaches that aggregate noise from individual data owners.
- Our algorithm is validated on real human activity datasets against other recently proposed empirical risk minimization algorithms on Distributed learning; whiles alternating the number of data owners and volumes of the local dataset. We empirically show the effectiveness of the proposed protocol for an extended privacy level. Our simulations indicate the practicality and feasibility of our model and are very close to the non-private classifier relative to the accuracy of the classifiers and their generalization errors.

In Section 2, we provide an outline of the related works. Section 3 presents some preliminaries and the definition of multi-party Differential privacy in the distributed domain. The proposed architecture is given in Section 4. Experimental results for the proposed architecture will be demonstrated in Section 5, Section 6 deals with the comparative evaluation of our algorithm.

2. Related works

Distributed machine learning (DML) [16] as a decentralized machine learning theory enables distributed training on a large scale of a dataset in edge devices including electronic meters, and sensors smartphones where no individual node is capable of getting the intelligent decision from a massive dataset within an appreciable period of time. DML technique has earned a remarkable reputation in numerous pragmatic areas such as visual object detection, health records, big data analysis, control policies, and medical text extraction. Regrettably, as the number of distributed data owners increases, the guarantee for the security of the datasets from the individual data owners becomes extremely difficult. This lack of security will increase the threat that adversaries attack the dataset preceded by the manipulation of the intermediate training result. Therefore, affecting data integrity which is a key component in training machine learning models. Adversarial data attacks [17] is one of the distinctive ways with the aim of corrupting the machine learning models by contaminating data during the training phase. Consider in a scenario where newly generated datasets are expected to be updated periodically by the data owners for improving the models, the adversary is likely to gain more chances of poisoning the dataset, posing a severe threat in the Distributed machine learning models. This kind of threat is considered one of the most imperative emerging security threats against machine learning models. Since the adversarial attack has the potential of misleading the diverse machine learning methods, a widely applicable DML protection mechanism is urgently required to be investigated. There have been numerous works conducted on privacy-preserving DML, most of the research approaches were greatly stimulated by privacy-preserving machine learning and data mining. The existing literature on privacy-preserving DML basically falls into two major categories: cryptography-based technique and perturbation-based methods.

The cryptography-based methods typically incorporate cryptographic tools to preserve the privacy of the datasets. Secure multiparty computation may potentially address these security threat in the

DML system. Though acquiring information with the aggregation of the dataset from multi-parties is a critical task for machine learning, in a real-world business setting, the prevention of privacy leakages while carrying out this privacy-preserving task is a very crucial requirement for secure multiparty computation. Secure multi-party computation problem refers to collaborative execution of a statistical function together by multiple data owners. After the computation, individual data owners acquire accurate results and no one can get more knowledge than the dataset inferred from the public intermediate results. Secure multiparty algorithms are basically cryptographic-based methods that apply a typical cryptographic technique to perform these Distributed machine learning tasks. The data owners try not to expose any knowledge on original data except that can be inferred from the output [7] of the Distributed machine learning task. Over the past few years, secure multiparty computation has widely been applied to achieve privacy-preserving in the distributed machine since it is more effective and efficient than other privacy-preserving algorithms. Secure MPC is capable of supporting floating-point and fix-point arithmetic operations [18], this arithmetic functions can be executed with controlled linear complexity [19]. Owing to these benefits, exploring the potential of secure multiparty computation required for privacy-preserving in Distributed machine learning has gained considerable attention over the past few years. Initial proposals to secure two-party(2PC) computation was first introduced by Yao [20] in 1982. Subsequently, Goldreich et al. [21] generalized and stretched 2PC method to the secure multiparty computer (MPC) problem. Secure MPC later gains so much research attention to finding practical ways of exploring the potential in this domain. Gentry [8] with the aid of homomorphic encryption with ideal lattices primitive was the first to introduce secure MPC. This was later preceded by numerous researchers proposing various secure MPC implementations, including Lost-cost Multi-party Computation for Dishonest Majority [22] Semi-homomorphic Encryption and Active-Secure Two-Party Computation [25]. To the highest degree, these algorithms can be categorized into two major methods such as secret sharing and homomorphic encryption. Gentry et al. [8] achieve the initial scheme with multiplicative and additive homomorphism respectively, this will require a long period of time to execute the complex circuits during the performance of the inevitable elimination of the noise. To the contrary, secrete sharing primitive [24] is capable of calculating infinite times of any multiplication and addition with an additional exchange of datasets. In a typical example of a two-party domain, Bansal et al. [26] applied secure scalar and secret sharing to protect privacy leakages during the training process which is not trivial to be extended to the secure multi-party models. Yuan et al. [27] propose a privacy-preserving back-propagation algorithm for secure multi-party deep learning over arbitrarily partitioned datasets grounded on BGN homomorphic encryption [28]. Nevertheless, the primitive requires all the data owners to be online and interactively collaborate to decrypt the ciphertext of the intervening parameters during each iteration. In [29], Hesamifard et al. propose a privacy-preserving machine learning algorithm using encrypted data to make encrypted predictions in the cloud. Since fully homomorphic encryption(FHE) [8] generates high computational complexities, they proposed a confidentially binary classification-based method to find a trade-off between the degree of the polynomial approximation and the secure performance of the training model. Li et al. [30] with the aid of multi-key fully homomorphic encryption (MK-FHE) [31] also propose a privacy-preserving multi-party deep learning primitive, in this setting, the individual data owners encrypts their datasets with different public keys and outsource them to the cloud server, the cloud server therefore train the deep learning classifiers with the application of MK-FHE. Based on the relevant literature above, it is obvious that most of the cryptography-based algorithms use fully homomorphic or multi-key fully homomorphic encryption primitives to encrypt the entire dataset before outsourcing it to the cloud server.

With the addition of noise to the raw dataset, the perturbation-based method is able to protect the privacy of the dataset. Agrawal et al. [32] proposes an algorithm that injects elaborately designed noise to the training data while preserving the statistical properties to enable the training of Naive Bayes classifier. With the gradual explosion of the digitized dataset, Fong et al. [33] offered a privacy-preserving learning algorithm by transforming the original dataset into groups of unreal datasets whiles preserving the accuracy for the learning model. Furthermore, this algorithm ensures that the original data samples cannot be reconstructed without the whole group of constructed datasets. DP is a strong golden standard to guarantee privacy-preserving for algorithms on aggregated datasets, which is widely applied in privacy-preserving DML to ensure that the dominance of any single data owners record is insignificant. DP has been utilized in many existing applications by large-scale businesses such as US Census Bureau [34]. A typical Distributed machine learning strategy applied in this domain is Empirical Risk Minimization (ERM), where the average error of the trained model over the aggregated datasets is minimized. There have been numerous proposals to advance the works on privacy-preserving algorithms for ERM problems with the application of variations of differential privacy. This paradigm is known as Differentially Private Empirical Risk Minimization (DP-ERM) [13]. DP-ERM reduces the empirical risk whiles providing the assurance the intermediate results of the learning model is differentially private based on the aggregated training dataset. This privacy-preserving guarantee ensures strong protection against potential adversaries such as inference attacks. To guarantee privacy-preserving in this domain, it is always essential to launch randomness to the training protocol. Based on the time for noise injection, there are mainly three ways to initiate randomness: objective perturbation, output perturbation, and gradient perturbation. This work introduces a differentially-private (DML) algorithms with the application of both gradient perturbation and output perturbation whiles injecting the noise within the secure multi-party computation.

3. Preliminaries and problem definition

In this section, we introduce the notations (Table 1) in our proposed protocol and the necessary background for our analyses, including empirical risk minimization,zero-concentrated differential privacy, and basic assumptions in secure multi-party computation.

3.1. Problem setting

Given a dataset $D = \{d_1, \cdots, d_n\}$ from a data universe $\mathcal{X}$ and a closed convex set $C \subseteq \mathbb{R}^p$, DP-ERM is to find $x_{\text{priv}} \in C$ so as to minimize the empirical risk, i.e.,

$$F^r(x, D) = \frac{1}{n} \sum_{i=1}^{n} f(x, z_i) + r(x), \tag{3.1}$$

with the guarantee of being differentially private, where f is the loss function and r is some simple (non)smooth convex function called regularizer. When the inputs are drawn i.i.d from an unknown

Table 1. Notations in our proposed architecture.

Notations	Description
D	Database of n records
$(\mathbf{x}_i, y_i)$	The i-th record in database D
ϑ	The parameter vector of neural networks
ϑ^*	The optimal model parameter ϑ
$\mathcal{L}(\vartheta)$	The loss function on database D
ϵ	The privacy budget of neural networks
R_j	Average relevance
Δ	Sensitivity
$\text{Lap}(\cdot)$	Laplace distribution
$g(\mathbf{x}_i)$	Gradients
$\tilde{g}(\mathbf{x}_i)$	The noisy gradients
α	Relevance ratio

underlying distribution $\mathcal{P}$ on $\mathcal{X}$, we also consider the population risk $\mathbb{E}_{z\sim\mathcal{P}}[f(x,z)]$. If the loss function is convex, the utility of the algorithm is measured by the expected excess empirical risk, i.e.,

$$\mathbb{E}_{\mathcal{A}}\left[F^r\left(x_{\text{priv}}, D\right)\right] - \min_{x\in C} F^r(x, D), \tag{3.2}$$

or the expected excess population risk (i.e., generalization error), i.e.,

$$\mathbb{E}_{z\sim\mathcal{P},\mathcal{A}}\left[f\left(x_{priv}, z\right)\right] - \min_{x\in C} \mathbb{E}_{z\sim\mathcal{P}}[f(x,z)], \tag{3.3}$$

where the expectation of $\mathcal{A}$ is taking over all the randomness of the algorithm.

3.2. Differential privacy

Let $D = \{d_1, d_2, ..., d_n\}$ represent n data points, each derived from some setting $\mathcal{D}$. Two neighboring databases D and $D^{'}$; if $|D| = |D^{'}|$ differing in exactly one data point. $D^{'}$ is obtained by the addition or removal of one observation from D. The concept of DP was commenced by Dwork [5] and outlined as follows:

Definition 1. *(ϵ, δ)-DP [5]. A randomized mechanism $\mathcal{M}$ satisfy (ϵ, δ)-DP if for every event $\mathcal{S} \subseteq$ range $(\mathcal{M})$ and for all $D, D^{'} \in D^n$,*

$$Pr[\mathcal{M}(D) \in S] \leq \exp(e) Pr\left[\mathcal{M}\left(D^{'}\right) \in S\right] + \delta \tag{3.4}$$

when $\delta = 0$, $\mathcal{M}$ accomplishes pure DP by providing stronger privacy protection than approximate DP with $\Delta > 0$. We can add noise sampled form Guassisan and Laplace distributions respectively to achieve ϵ-DP and (ϵ, δ)-DP where the noise is proportional to ℓ_2 norm sensitivity of $\mathcal{M}$; given as $\Delta\mathcal{M} = ||\mathcal{M}(D) - \mathcal{M}(D')||$.

Definition 2. *($\ell_1$and ℓ_2 norm sensitivity) Let $q : D^n \leftarrow \mathbb{R}^d$ be a query function. The ℓ_1(resp. ℓ_2) sensitivity of q, denoted by $\Delta_1(q)$ (resp., $\Delta_2(q)$) is defined as follows:*

$$\Delta_1(q) = \max_{D \sim D} \left\| q(D) - q\left(D'\right) \right\|_1, \quad \Delta_2(q) = \max_{D \sim D} \left\| q(D) - q\left(D'\right) \right\|_2 \tag{3.5}$$

The ℓ_1 and ℓ_2 sensitivities represent the maximum change in the output value of q (over all possible neighboring databases in D^n) when one individual's data is changed.

Theorem 1. *Let $\epsilon \in (0, 1)$ be arbitrary and q be a query function with ℓ_2 sensitivity of $\Delta_2(q)$. The Gaussian Mechanism, which returns $q(D) + N(0, o^2)$ Let $\epsilon \in (0, 1)$ be arbitrary and q be a query function with ℓ_2 sensitivity of $\Delta_2(q)$. The Gaussian Mechanism [35], which returns $q(D) + N(0, \sigma^2)$ with*

$$\sigma \geq \frac{\Delta_2(q)}{\epsilon} \sqrt{2 \ln(1.25/\delta)} \tag{3.6}$$

is (ϵ, δ)-DP

A critical property of DP is its privacy guarantee reduces gracefully under the composition. The most basic composition result shows that the privacy loss grows linearly under k-fold composition [36]. This implies, if we sequentially apply an (ϵ, δ)-differential privacy algorithm n times on the same data, the resulting process is $(n\epsilon, n\delta)$. Dwork et al. [37] provided a booting method to construct an improved privacy-preserving synopsis on the queries with an advanced composition; the loss function upsurges sub-linearly at the rate of $\sqrt{n}$.

Theorem 2. *For all $\epsilon, \delta, \delta' \geq 0$ the class of (ϵ, δ)-differential private mechanisms satisfy $(\epsilon', n\delta + \delta')$-differential privacy under k-fold adaptive composition for $\epsilon' = \sqrt{2n} In(\frac{1}{\delta'})\epsilon + n\epsilon(e^{\epsilon - 1})$ as stated in the advance composition [37].*

3.3. Zero-concentrated differential privacy

Whiles, differential privacy is suitable for algorithms such as output perturbation, it is not the preferred choice for gradient perturbation which is essentially repeated sampling of statistical noise during the iterative learning process. Bun and Stainke [15] provided zero-concentrated DP (zCDP). which has a tight composition bound and a preferable option for gradient perturbation. We define ρ-zCDP by the introduction of the privacy loss random variable as applied in the definition of zCDP.

Definition 3. *For an output $0 \in range(\mathcal{M})$, the privacy loss random variable $\mathcal{Z}$ of the mechanism $\mathcal{M}$ is defined as follows:*

$$Z = \log \frac{\mathbb{P}[\mathcal{M}(D) = \circ]}{\mathbb{P}\left[\mathcal{M}\left(D'\right) = \circ\right]} \tag{3.7}$$

ρ-zCDP therefore imposes a bound on the moment generating function of the privacy loss $\mathcal{Z}$ and requires it to be tightly concentrated around zero mean, hence it is unlikely to distinguish $\mathcal{D}$ from $\mathcal{D}'$. Formally, it important to satisfy the following:

$$e^{D_\alpha(M(D) \| \mathcal{M}(D'))} = \mathbb{E}\left[e^{(\alpha-1)Z}\right] \leq e^{(\alpha-1)\alpha\rho}, \forall \alpha \in (1, \infty) \tag{3.8}$$

where $D_\alpha\left(M(D) \| \mathcal{M}\left(D'\right)\right)$ is the α-Rényi divergence. In this work, we apply the resulting zCDP composition.

Lemma 1. *[15] If two mechanisms satisfy ρ_1 -zCDP and ρ_2 -zCDP, then their composition satisfy $(\rho_1 + \rho_1)$-zCDP*

If two mechanisms satisfy ρ_1 -zCDP and ρ_2 -zCDP, then their composition satisfy $(\rho_1 + \rho_2)$-zCDP

Lemma 2. *[15] The Gaussian mechanism returns $q(\mathcal{D}) + \mathcal{N}(0, \sigma^2)$ satisfies $\Delta_2(q)^2/(2\sigma^2)$-zCDP*

Lemma 3. *[15] If $\mathcal{M}$ satisfies ϵ-DP, then $\mathcal{M}$ satisfy $(\frac{1}{2}\epsilon^2)$-zCDP, then $\mathcal{M}$ is $(\rho + 2\sqrt{\rho \log(1/\delta)}, \delta)$-DP for any $\delta > 0$.*

3.4. Secure multi-party computation

In our security threat model, we consider honest-but-curious (semi-honest) data providers who wish to collaboratively train a model without exposing their individual inputs to other data owners. Data providers do not collude to temper with the collaborative functionality or inject garbage input data, they are capable of passively inferring about inputs of other data providers depending on the implementation of the algorithm. We applied generic secure multiparty computation primitives to securely aggregate locally trained classifiers and their gradients. K. Owusu-Agyemang et al. [38] demonstrated the secure aggregation of multiple individual datasets and locally trained models. This method will enable our model to have a secure verifiable computation delegation from the aggregated locally trained models. Therefore helping the data owners to also update their locally trained models with higher accuracy improvement. In this paper, we can use this method to achieve our secured multi-party model aggregation. For circumstances where there is a high risk of collusion, numerous secure multi-party protocols can be used to an individual honest data provider even if all other data owners are malicious. The focus of this paper is not to improve or evaluate the execution of the secure multiparty computation, since our proposed algorithm is capable of been implemented using well know secured multiparty computation algorithms.

3.5. Multi-party machine learning

We demonstrate our OP and GP methods with the theoretical analysis of DP and generalization error bound. The following ERM objective is considered:

$$R_D(\theta) = \frac{1}{n} \sum_{i=1}^{n} \ell(\theta, x_i, y_i) + \lambda N(\theta) \tag{3.9}$$

where $\ell(\theta)$ is a convex loss function that is G-Lipschitz and L-smooth over $\theta \in \mathbb{R}^d$. $N(\cdot)$ is the regularization term. We consider $R(\cdot)$ to be λ-strongly convex. Individual data instance $(x_i; y_i) \in D$ lies in a unit ball. For an individual j, with dataset D_j of size n_j, we denote its data instance as (x_i^j, y_i^j).

3.6. Synthesizing coupling for Noisy Max Report

Given $\varphi = \{w_1, w_2, ..., w_n\} \in \mathbb{R}^n$ and $f : \mathbb{R}^n \to \mathbb{R}$ as a function that implicitly depends on $\mathcal{D}$. In cases where we want to pick a point $w_i \in \varphi$ with highest $\ell(w_i, \mathcal{D})$. An algorithm (ϵ)-DP called Report Noisy Max Mechanism [36] injects independent statistical noise from $\text{Lap}(\triangle_1(\ell/\epsilon))$ to each $\ell(w_i)$, for $i \in [n]$, whiles returning the index i of the maximum value i.e.,

$$i = \arg\max_{j\in[n]}\{\ell(\mathbf{w}_j) + \mathrm{Lap}(\Delta_\ell/\epsilon)\}$$

with Lap(λ) denoting a Laplace noise allocation with 0 mean and scale parameter λ; the notation $[n]$ is used to denote the set $\{1, 2, 3, ...n\}$. Although Report Noisy Max is ϵDP for arrays of any length; and it was originally considered to operate with pure ϵ-DP, it has also been affected by inaccurate privacy proofs in lots of previous proposals. To prove this stronger guarantee, it is essential to apply a more sophisticated coupling strategy [39]. To enable [39] to work with ρ-zCDP Lemma 3 conversion result is applied. Hence the ϵ-differential private protocol satisfies $\frac{\epsilon^2}{2}$-zCDP. Consequently, anytime we wish to use zCDP, we assign $\rho^{'}$ of the privacy budget to Coupling Strategies, we represent the Coupling Strategies by $\epsilon = \sqrt{2\rho'}$.

Algorithm 1: Coupling Strategies ($\varphi, \Delta_1(\ell), \epsilon$)

```
Input: $\varphi$: a set of data entities, $\Delta_1\ell$: sensitivity of $\ell$, $\epsilon$ : privacy budget for pure $\epsilon$-DP
$\hat{\varphi} = \{\hat{v}_i = v + Lap(\Delta_1(\ell)/\epsilon) : v \in \varphi, i \in \epsilon[|\varphi|]\}$;
Return: argmax$_{j\in[|\varphi|]}\ \hat{v}_j$
```

3.7. Gradient estimation for zCDP

An algorithm for the recycling of the gradients estimates that were not useful during the parameter updates will be applied in our main protocol. At iteration r we will use $\rho_r^{'}$-zCDP privacy budget for the estimation of the privacy budget. If $\Delta_2(\Delta\ell) = L_2$ sensitivity of the gradients of ℓ then, we can then measured as $G_r = \Delta\ell(w_r) + N(O, \frac{\Delta_2(\Delta\ell)^2}{2\rho_r})$ A larger share of privacy budget $\rho_{r+1} > \rho_r$ is triggered if the accuracy is not enough. Another independent measurement is initiated using $\rho_{r+1} - \rho_r$ privacy budget $G_r^{'} = \Delta\ell(w_r) + N(O, \frac{\Delta_2(\Delta\ell)^2}{2(\rho_{r+1}-\rho_r)})$. Therefore $G_r + G_r^{'} = \hat{G}_r = \frac{\rho_r G_r + (\rho_{r+1}-\rho_r)G_r^{'}}{\rho_r + (\rho_{r+1}-\rho_r)}$.

We demonstrate the estimated gradient as : $E[\hat{G}_t] = \nabla\ell(\mathbf{w}_r)$

$$Var(\hat{G}_r) = (\rho_r^2\frac{\Delta_2(\Delta\ell)^2}{2\rho_r} + \frac{\Delta_2(\Delta\ell)^2}{2(\rho_{r+1}-\rho_r)}(\rho_{r+1}-\rho_r)^2)/\rho_{r+1}^2 = \frac{\Delta_2(\Delta\ell)^2}{2\rho_{r+1}}$$

4. Our proposed architecture

4.1. Model aggregation with output perturbation:

In our proposed distributed machine learning protocol, we extend the differential privacy bound of [40] for the output perturbation algorithm, where adequate noise is injected to preserve the privacy of individual data owners and final output throughout the learning process. Our model aggregation with the output the perturbation model is represented in Figure 2.

Theorem 3. *In our aggregated model estimator,* $\hat{\theta} = \frac{1}{m}\sum_{j=1}^{m}\hat{\theta}^{(j)}$ *where* $\widehat{\theta^{(j)}} = \arg\min_\theta \frac{1}{n_j}\sum_{i=1}^{n_j}\ell\left(\theta, x_i^{(j)}, y_i^{(j)}\right) + \lambda N(\theta)$ *with an optimal model estimator* θ^* *learning from the*

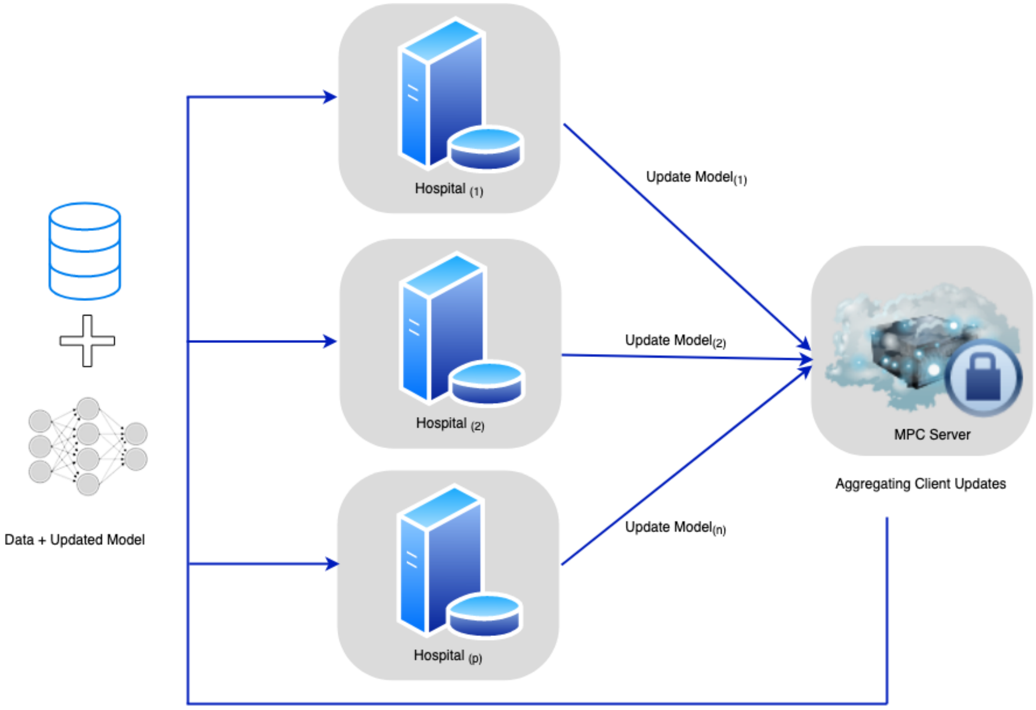

Figure 2. Workflow of our multi-scheme output perturbation method.

centralized individual dataset such that the data reside in a unit ball and $\ell(\cdot)$ is G -Lipschitz, we therefore obtain:

$$\|\widehat{\theta} - \theta^*\| \leq \frac{G(m-1)}{n_{(1)}\lambda} \tag{4.1}$$

Proof. For an individual data owner P_j, the local model estimator is given as:

$$\widehat{\theta}^{(j)} = \arg\min_{\theta} \frac{1}{n_j} \sum_{i=1}^{n_j} \ell\left(\theta, x_i^{(j)}, y_i^{(j)}\right) + \lambda N(\theta) = \arg\min_{\theta} G(\theta)$$

Therefore the centralized model estimator is stated as:

$$\theta^* = \arg\min_{\theta} \frac{1}{n_j} \sum_{i=1}^{n_j} \ell\left(\theta, x_i^{(j)}, y_i^{(j)}\right) + \sum_{l\neq j} \frac{1}{n_l} \sum_{i=1}^{n_l} \ell\left(\theta, x_i^{(l)}, y_i^{(l)}\right) + \lambda N(\theta) = \arg\min_{\theta} G(\theta) + g(\theta)$$

The values of g_1 and G_2 are represented as follows:

$$\begin{aligned} g_1 &= \max_\theta \|\nabla g(\theta)\| = \max_\theta \textstyle\sum_{l\neq j} \frac{1}{n_l} \left\|\nabla \ell\left(\theta, x_i^{(l)}, y_i^{(l)}\right)\right\| \leq G \textstyle\sum_{l\neq j} \frac{1}{n_l} \\ G_2 &= \min_v \min_\theta \left\|v^\top \nabla^2 G(\theta) v\right\| = \min_v \min_\theta \left\|v^\top \left(\frac{1}{n_j}\left\|\nabla^2 \ell\left(\theta, x_i^{(j)}, y_i^{(j)}\right)\right\| + \lambda.1\right) v\right\| \geq \lambda \end{aligned}$$

With the application of Lemma [1] *of Chaudhuri and Monteleoni [40] we obtain* $\|\widehat{\theta}^{(j)} - \theta^{*}\| = \frac{G}{\lambda}\sum_{l\neq j}\frac{1}{n_l}$. *With the application of triangle inequality, we have:*

$$\left\|\widehat{\theta} - \theta^{*}\right\| \leq \frac{1}{m}\sum_{j}\left\|\hat{\theta}^{(j)} - \theta^{*}\right\| = \frac{G}{m\lambda}\sum_{j}\sum_{l\neq j}\frac{1}{n_l} = \frac{G(m-1)}{m\lambda}\sum_{j}\frac{1}{n_j} \leq \frac{G(m-1)}{n_{(1)}\lambda}$$

In minimizing the local objective function $R_D(\theta) = \frac{1}{n}\sum_{i=1}^{n}\ell\left(\theta, x_i, y_i\right) + \lambda N(\theta)$, we obtain $\widehat{\theta}^{(j)}$ as its corresponding local model estimator.

$$\widehat{\theta}_{priv} = \frac{1}{k}\sum_{j=1}^{k}\widehat{\theta}^{(j)} + \eta \tag{4.2}$$

is the perturbed aggregate model estimator; where η is the Laplace noise injected into an aggregated model estimator to obtain DP. We, therefore, adopt K.Owusu-Agyemang et al. [38] secure model aggregation for our secure MPC model. The theory below administers a bound on the quantity of noise required to attain DP.

Theorem 4. *If* $\widehat{\theta}_{priv} = \frac{1}{k}\sum_{j=1}^{k}\widehat{\theta}^{(j)} + \eta$ *is the perturbed aggregate model estimator whiles* $\widehat{\theta}^{(j)} = \arg\min_{\theta}\frac{1}{n_j}\sum_{i=1}^{n_j}\ell\left(\theta, x_i^{(j)}, y_i^{(j)}\right) + \lambda P(\theta)$ *with the data reside in a unit ball and* $\ell(\cdot)$ *is G-Lipschitz , then* $\widehat{\theta}_{priv}$ *is* ϵ*-differentially private if :* $\eta = \mathrm{Lap}\left(\frac{2G}{kn_{(1)}\lambda\epsilon}\right)$

$n_{(1)}$ represent the volume of the minimum data set amid the k data owners, regularization parameter λ and DP budget ϵ.

Proof. As there are k entities representing one record of data owner j altered in the neighboring datasets formally:

$$\frac{\Pr(\widehat{\theta}|D)}{\Pr\left(\widehat{\theta}|D'\right)} = \frac{\Pr\left(\frac{1}{k}\sum_{i\neq j}\widehat{\theta}^{(i)} + \frac{1}{k}\widehat{\theta}^{(j)} + \eta|D\right)}{\Pr\left(\frac{1}{k}\sum_{i\neq j}\widehat{\theta}^{(i)} + \frac{1}{k}\widehat{\theta}'^{(j)} + \eta|D'\right)} = \frac{\exp\left[\frac{k\cdot n_{(1)}\epsilon\lambda}{2G}\frac{\|\widehat{\theta}^{(j)}\|}{k}\right]}{\exp\left[\frac{k\cdot n_{(1)}\epsilon\lambda}{2G}\frac{\|\widehat{\theta}^{(j)}\|}{k}\right]} \leq \exp\left[\frac{n_{(1)}\epsilon\lambda}{2G}\left\|\widehat{\theta}^{(j)} - \widehat{\theta}'^{(j)}\right\|\right]$$
$$\leq \exp\left[\frac{n_{(1)}\epsilon\lambda}{2G}\frac{2G}{n_j\lambda}\right] \leq \exp(\epsilon)$$

Provision of a bound on the excess empirical risk and true risk is similar to [12] and [13] with our bounds tighter than both of them as we demand very fewer DP noise.

Theorem 5. *If a perturbed aggregated model estimator* $\widehat{\theta}_{priv} = \frac{1}{m}\sum_{j=1}^{m}\widehat{\theta}^{(j)} + \eta$ *where* $\widehat{\theta}^{(j)} = \arg\min_{\theta}\frac{1}{n_j}\sum_{i=1}^{n_j}\ell\left(\theta, x_i^{(j)}, y_i^{(j)}\right) + \lambda N(\theta)$ *and an optimum model estimator* θ^{*} *learning from the centralized data such that the data reside in a unit ball and* $\ell(\cdot)$ *is G -Lipschitz and L -smooth, then the bound on excess empirical risk is given as:*

$$R(\widehat{\theta}_{priv}) \leq R(\theta^{*}) + A_1\frac{G^2(\lambda + L)}{n_{(1)}^2\lambda^2}\left(m^2 + \frac{d^2\log^2(d/\delta)}{m^2\epsilon^2} + \frac{d\log(d/\delta)}{\epsilon}\right)$$

where A_1 *is an absolute constant.*

Proof. With the application of Taylor's Expansion, we therefore obtain:

$$R(\widehat{\theta}_{priv}) = R(\theta^{*}) + (\widehat{\theta}_{priv} - \theta^{*})\nabla R(\theta^{*}) + \frac{1}{2}(\widehat{\theta}_{priv} - \theta^{*})\nabla^{2}R(\theta)(\widehat{\theta}_{priv} - \mid \theta^{*})$$

where $\theta = \alpha\widehat{\theta}_{priv} + (1-\alpha)\theta^{*}$ for some $\alpha \in [0,1]$. By definition, $\nabla R(\theta^{*}) = 0$, thus we get

$$R(\hat{\theta}^{priv}) - R(\theta^{*}) \leq \frac{1}{2}\|\widehat{\theta}_{priv} - \theta^{*}\|^{2} \cdot \|\nabla^{2}J(\theta)\|$$

since $\ell(\cdot)$ is L -smooth, we have $\left\|\nabla^{2}J(\theta)\right\| \leq \lambda + L$, therefore

$$\begin{aligned} R(\widehat{\theta}_{priv}) &\leq R(\theta^{*}) + \frac{\lambda+L}{2}\|\widehat{\theta} - \theta^{*} + \eta\|^{2} \leq R(\theta^{*}) + \frac{\lambda+L}{2}[\|\widehat{\theta} - \theta^{*}t\|^{2} + \|\eta\|^{2} + 2(\widehat{\theta} - \theta^{*})^{\top}\eta] \\ &\leq R(\theta^{*}) + \frac{\lambda+L}{2}[\|\widehat{\theta} - \theta^{*}\|^{2} + \|\eta\|^{2} + 2\|\widehat{\theta} - \theta^{*}\| \cdot \|\eta\|] \end{aligned}$$

Theorem 6. *If a perturbed aggregated model estimator* $\widehat{\theta}_{priv} = \frac{1}{k}\sum_{j=1}^{k}\widehat{\theta}^{(j)} + \eta$ *where* $\widehat{\theta}^{(j)} = \arg\min_{\theta}\frac{1}{n_j}\sum_{i=1}^{n_j}\ell\left(\theta, x_i^{(j)}, y_i^{(j)}\right) + \lambda P(\theta)$ *and an optimum model estimator* θ^{*} *trained on the centralized data to this extent dataset reside in a unit ball and* $\ell(\cdot)$ *is G-Lipschitz and L-smooth, then the bound on excess empirical risk is grounded on probability at minimum* $1-\gamma$*:*

$$\mathbb{E}[\widetilde{R}(\widehat{\theta}_{priv})] - \min_{\theta}\widetilde{R}(\theta) \leq C_1\frac{G^{2}(\lambda+L)}{n_{(1)}^{2}\lambda^{2}}(m^{2} + \frac{d^{2}\log^{2}(d/\delta)}{m^{2}\epsilon^{2}} + \frac{d\log(d/\delta)}{\epsilon}) + C_2\frac{G^{2}\log(1/\gamma)}{\lambda n}$$

where n is the volume of the centralized dataset. $\widetilde{R}(\theta) = \mathbb{E}_{x,y}[\ell(\theta,x,y)] + \lambda N(\theta), A_1, A_2$ *are absolute constants, and the expectation is taking relative to the noise* η*.*

4.2. Gradient perturbation with adaptive iteration privacy budget

We give considerable attention to a centralized private empirical risk minimization to adopt per-iteration privacy budget for k entities, with individual data set $\mathcal{D}_j$ of volume n_j of independent observations.

$$R_D(\theta) = \min_{\theta}\frac{1}{m}\sum_{j=1}^{m}\frac{1}{n_j}\sum_{i=1}^{n_j}\ell(\theta, x_i^{(j)}, y_i^{(j)}) + \lambda N(\theta) \tag{4.3}$$

Data owners can collaboratively train a differentially private classifier by adopting the per-iteration privacy budget by the addition of noise to the aggregated gradient inside secure MPC to make individual iteration progress towards an optimal solution. It is imperative to consider that the regularization expression in Eq (4.3) has no privacy guarantee and does not have any privacy implications since it is independent of the data sets. Our adaptive iterative gradient perturbation method is represented in Figure 3.

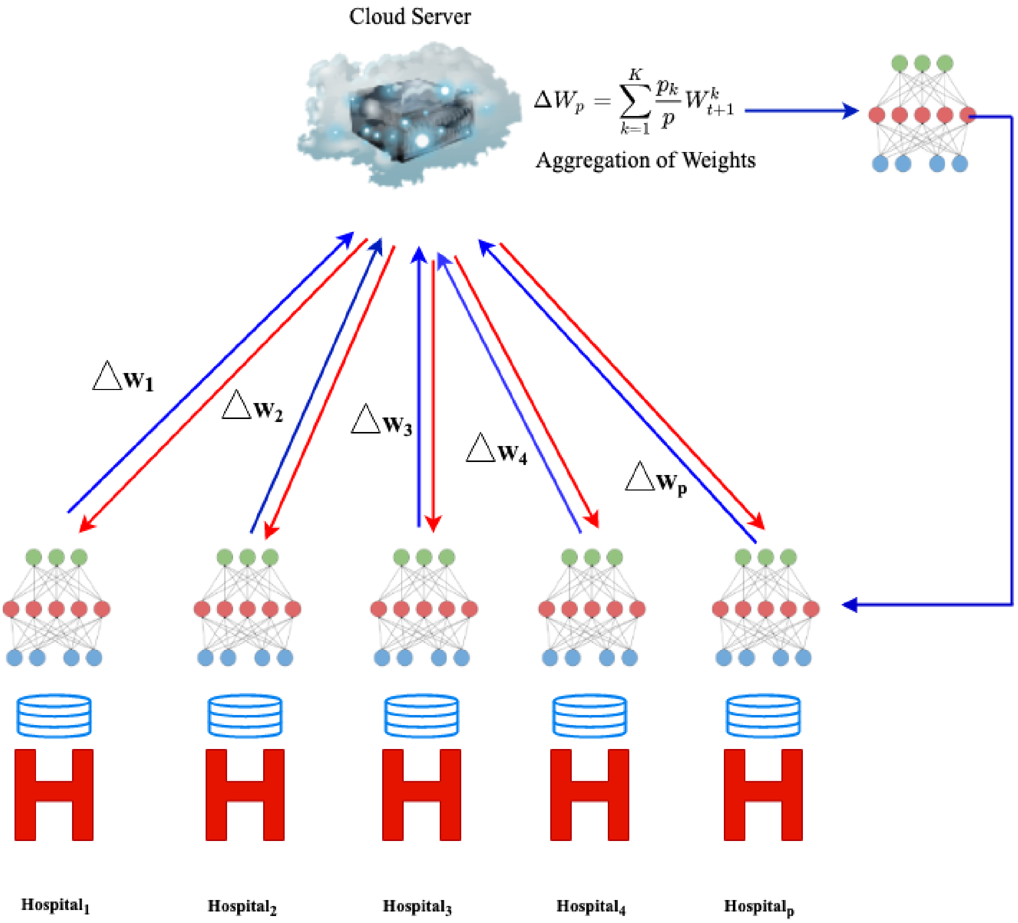

Figure 3. Gradient perturbation workflow.

Theorem 7. *With a Distributed model estimator θ_T attained by minimizing $J_{\mathcal{R}}(\theta)$ followed by T iterations of our gradient descent method executed collaboratively by k participants individually possessing dataset D^j of size n_j with each data instance $\{d_1, d_2, d_n\} \in D^j$ reside in a unit ball and $\ell(\theta)$ is G-Lipschitz and L-smooth above $\theta \in A$. $\frac{1}{L}$ as the learning rate whiles gradients are perturbed with statistical noise using the Gaussian mechanism with variance σ^2 in $z \in \mathcal{N}(O, \sigma^2 I)$, then θ_T is $(\epsilon_{tot}, \delta_{tot})$-differentially private if:*

$$\sigma^2 = \frac{8G^2 T \log(1/\delta)}{m^2 n_{(1)}^2 \epsilon^2} \tag{4.4}$$

with n_i been the least data volume amid the individual k participants.

Proof. With initial gradient at step i

$$\hat{G}_t = \nabla J(w, D) + \mathcal{N}(0, \sigma^2 I_p) = \frac{1}{m} \sum_{j=1}^{m} \frac{1}{n_j} \sum_{i=1}^{n_j} \nabla \ell(w, x_i^{(j)}, y_i^{(j)}) + \mathcal{N}(0, \sigma^2 I_p)$$

The magnitude of the Gaussian noise σ^2 on the highest impact an individual can exhibit on g_t which is measured by $\Delta_2(g)$. To bound $\Delta_2(g)$ quantity, we apply the gradient clipping method of [41] to compute the gradient $\nabla\ell(w, x_i^{(j)}, y_i^{(j)})$ for $\{i = 1, 2..., n\}$ we clip the gradient in L_2-norm and divide it by Max(1, $\frac{\|\nabla\ell(w,x_i^{(j)},y_i^{(j)})\|_2}{A_g}$), compute the sum and add the Gaussian noise with the variance $\frac{A_g^2}{2\rho_{gm}}$ and eventually normalize it to a unit norm. That is to ensure L_2-sensitivity of the gradient is bounded by A_g to satisfy ρ_{gm}-zCDP by Lemma 2. In a secure MPC learning domain, since an algorithm cannot depend on a guarantee in expectation (i.e. $\mathrm{E}[\nabla\ell(\mathbf{w}_t; d_{i_t})|\mathbf{w}_t] = \nabla f(\mathbf{w}_t)$), it is important to efficiently apply per-iteration budget. We therefore deploy the privacy budget by testing if a given noisy estimate $\hat{g}_t$ of gradient is in a descent direction by applying a portion of the privacy budget ρ_{nmax} . Our algorithm then construct $\Omega = \{f(\mathbf{w}_t - \alpha\hat{g}_t) : \alpha \in \Phi\}$ where Ω represent the objective value evaluated at $\{\mathbf{w}_t - \alpha\hat{g}_t\}$ whiles Φ is the set of pre-defined step sizes. Then it decides which step volume yields the minimum objective value using the coupling strategy. We bound the sensitivity of ℓ by using the concept of gradient clipping to f objective function. With a specified fixed clipping threshold A_b, we then calculate $\ell(w_t; x_i, y_i)$, clipping the values greater than A_b to take the summation of the clipped values.

In cases where the direction $-\hat{g}_t$ is considered to be in a bad direction by the coupling strategy, our proposed protocol escalates the privacy budget for the estimation of the noisy gradient ρ_{gn} by a factor of $1 + \gamma$ We utilize the gradient averaging method to improve the validity of the gradient by subtracting ρ_0 from ρ_{gn} i.e(noisy gradient) to enable us to get the current gradient. The coupling strategy is applied to verify the new direction again. it is continuously applied until it returns a non-zero index i.e., attaining a decent direction.

Our proposed iterative gradient perturbation-based scheme is a composition of coupling Strategy ϵ, and $\frac{\epsilon^2}{2}$ as the basic tools to enable us to achieve diverse types of differential privacy; Gaussian mechanism on the other hand is also applied to provide zCDP. Algorithm 2 demonstrates the details of each step of our proposed gradient perturbation-based-algorithm.

Theorem 8. *We apply the conversion tools provided by Lemmas 2 and 3 to enable us to compare other algorithms that use approximated (ϵ, δ). Given (ϵ_T, δ_T)-DP as the total privacy budget and with the application of Lemma 3 we achieve the subsequent inequality for ρ:*

$$\epsilon_{\mathrm{T}} \geq \rho + 2\sqrt{\rho \log(1/\delta_{\mathrm{T}})} \tag{4.5}$$

With the overall privacy budget ρ for zCDP, our protocol vigorously calculates and subtracts the quantity of essential privacy budget whenever it requires access to the data sets throughout the run-time. This promises that the complete execution of our protocol meets ρ-zCDP. SGD method with continuous step sizes, in general, cannot assure the convergence to the optimal irrespective of how a strongly convex objective function can become. For this reason, the discrepancy in private gradient estimation is expected to be managed. In order to assure convergence, stochastic optimization methods basically implement the conditions $\sum_t \alpha_t^2 < \infty$ and $\sum_t \alpha_t = \infty$ based on their step size [42]. This will enable the differences in the updates to diminish progressively towards the optimal. Consequently, we monitor our step sizes chosen by the coupling strategy method and adaptively manage the scope of step sizes in Θ. We therefore initialize Θ with fairly spaced n points ranging from 0 and α_{max}. An update of $\alpha_{\max} = (1 + \eta)\max(\alpha_t, \alpha_{t-1}, \ldots, \alpha_{t-\tau+1})$ is performed at every iteration τ; with (α_t denoting the step size chosen at iteration t. Our algorithm is empirically observed to adaptively alter the scope of step sizes depending on the relative position of the present iteration to the optimal. The validity of our proposed scheme basically depends on ρ-zCDP composition which accounts for the cost of privacy for each primitive.

Theorem 9. *Algorithm 2 Meets ρ-zCDP and (ϵ_T, δ_T)-DP*

Proof. We expect values of (ϵ_T, δ_T) where no ρ-zCDP privacy budget is offered to our algorithm. Line 2 is capable of imagining the correct value of ρ to such a degree that ρ-zCDP can additionally satisfy frail (ϵ_T, δ_T). For our algorithm to achieve pure zCDP mode with the utilization of the privacy budget; Line 7 measures the noisy gradient, Line 12 performing the coupling strategy for noisy max whiles Line 18 is responsible for averaging the gradient. Furthermore, Line 3 guarantees that remaining privacy budget is always above 0 while Line 14 ensures our privacy budget is not exhausted. This is very critical to our algorithm since the weights are the output that is visible outside our proposed protocol. Our algorithm satisfies ρ-zCDP when all protocol operations apply the required share of the privacy budget allocated.

5. Performance analysis

We validate the performance of the simulation for our proposed algorithm for regression and classification tasks. Based on Wang et al. [43] method, we perform a pre-processing of the datasets. In our classification task, we apply a regularized logistic regression classifier over three (3) real-world datasets i.e., Adult [44], CICIDS2018 [45] and CICMalDroid2020 [46]. Table 2 represents the features of the datasets explored in the investigation.

In this domain, we predict if the interconnection is a denial-of-service(DoS) attack or otherwise. We indiscriminately sample 70,000 individual data along with dividing amongst training dataset of 50,000 records whiles the 20,000 records are used as a test set. With $\mathbf{x}_i \in \mathbb{R}^{p+1}, y_i \in \{-1, +1\}$, and $\lambda > 0$ as the regularization coefficient. Throughout our simulations; we set coefficient $\lambda = 0.001$, learning rate $\eta = 1$,failure probability $\theta = 0.001$,$\epsilon = 0.05$ privacy budget, G-Lipschitz constant = 1 and entire iterations $T = 1000$ for GD. We validate our proposed output perturbation and gradient perturbation-based algorithms with other benchmarks relative to optimality and relative accuracy loss. In the case of regression, relative accuracy loss is termed as mean square error (MSE) θ and θ^* which is the difference in accuracy over the test data.

5.1. Benchmark for comparison

In our proposed multi-party computation output perturbation-based model aggregation (MS-OP), we demonstrate the comparison of this model with Pathak et al. [12] which is represented as PAT, other cutting-edge differential privacy benchmarks are also achieved by the application of objective perturbation and output perturbation techniques of Wang et al. [43] on each of the locally trained model estimator $\widehat{\theta_j}$ to attain a differentially private local model estimator whiles aggregation of the classifier is computed to attain differentially private aggregated classifier $\widehat{\theta_{priv}}$ with confidence intervals for the parameters in the model. For our experiments on our proposed adaptive iterative gradient perturbation-based learning algorithm, we adopt a benchmark of aggregation for locally perturbed gradients [23] with the aim of improving the noise bound by applying zCDP and coupling strategy [39] also for the verification of the privacy budget. Our proposed multi-party computation output perturbation-based model aggregation and multiparty computation adaptive iterative gradient perturbation-based

Algorithm 2: Our proposed iterative adaptive gradient perturbation-based algorithm

```
   Input: privacy budget $\rho_{nmax}, \rho_g, \epsilon_T, \delta_T$,rate of budget increase $\gamma$ Clipping thresholds
          $A_b, A_g(x_i^{(j)}, y_i^{(j)}) \in D^{(j)} f(\mathbf{w}) = \sum_{i=1}^{n} \ell(\mathbf{w}; d_i)$G-Lipschitz constant = 1, learning rate$\eta = 1$,
          regularization coefficient$\lambda = 0.001$, privacy budget $\epsilon = 0.05$, $\delta = 0.001$ failure
          probability and overall iterations $T = 1000$
1  initialization $w_0$ and $\Theta$ ;
2  $t \leftarrow 0, \rho \rightarrow$ solve line (5) for $\rho$;
3  while $\rho$ >0 do
4      i ← 0;
5      $\mathbf{g}_t \leftarrow \sum_{i=1}^{n}(\nabla\ell(\mathbf{w}_t; d_i)/Max(1, \frac{\|\nabla\ell(w,x_i^{(j)},y_i^{(j)})\|_2}{A_g})$;
6      $\hat{g}_t \leftarrow \mathbf{g}_t + N(0, (A_{\rm g}^2/2\rho_{\rm gn})\mathbf{I})$;
7      $\rho \leftarrow \rho - \rho_{\rm gn}$;
8      $\hat{g}_t \leftarrow \hat{g}_t/\|\bar{\mathbf{g}}_t\|_2$;
9      while $i = 0$ do
10         $\Omega = f(\mathbf{w}_t - \alpha\hat{g}_t) : \alpha \in \Phi$;
11         $\rho \leftarrow \rho - \rho_{\rm nmax}$;
12         $i \leftarrow$ Coupling strategy $(-\Omega, A_{\rm b}, \sqrt{2\rho_{\rm nmax}})$;
13         if $i$ ¿ 0 then
14             $\mathbf{w}_{t+1} \leftarrow \mathbf{w}_t - \alpha_i\hat{g}_t$;
15         else
16             $\rho_{\rm o} \leftarrow \rho_{\rm gn}$;
17             $\rho_{\rm gn} \leftarrow (1+\gamma)\rho_{\rm gn}$;
18             $\hat{g}_t \leftarrow$ GradientAverage($\rho_{\rm o}$ ,$\boldsymbol{\rho}_{\mathbf{gn}}, \mathbf{g}_t, \hat{g}_t, A_{\rm g}$ );
19             $\rho \leftarrow \rho - (\rho_{\rm gn} - \rho_{\rm o})$;
20     $t \leftarrow t + 1$;
21 return $w_t$;
22 Function Gradient-Average(($\rho_o$ ,$\boldsymbol{\rho}_{\mathbf{h}}, \mathbf{g}_t, \hat{g}_t, A_g$ )):
23     $\hat{g}_2 \leftarrow$ g + $N(0, (\frac{A_{\rm g}^2}{2(\rho_h - \rho_{\rm o})})$I);
24     $\hat{S} \leftarrow \frac{\rho_{\rm o}\,\hat{g} + (\rho_h - \rho_{\rm o})\hat{g}_2}{\rho_h}$;
25     return $\hat{S}$;
26 end
```

Table 2. Summary of the datasets.

Dataset	Size (n)	Dimension
Adult [44]	48,842	124
CICIDS2018 [45]	16,000,000	125
CICMalDroid2020 [46]	17,341	470

frameworks is represented as MS-OP and MS-GP respectively (with the application of Algorithm 2).

In all our simulations there is a variation of the number of data owners p from 100–1000 with up to 50,000 data owners with each of them possessing only one data instance.

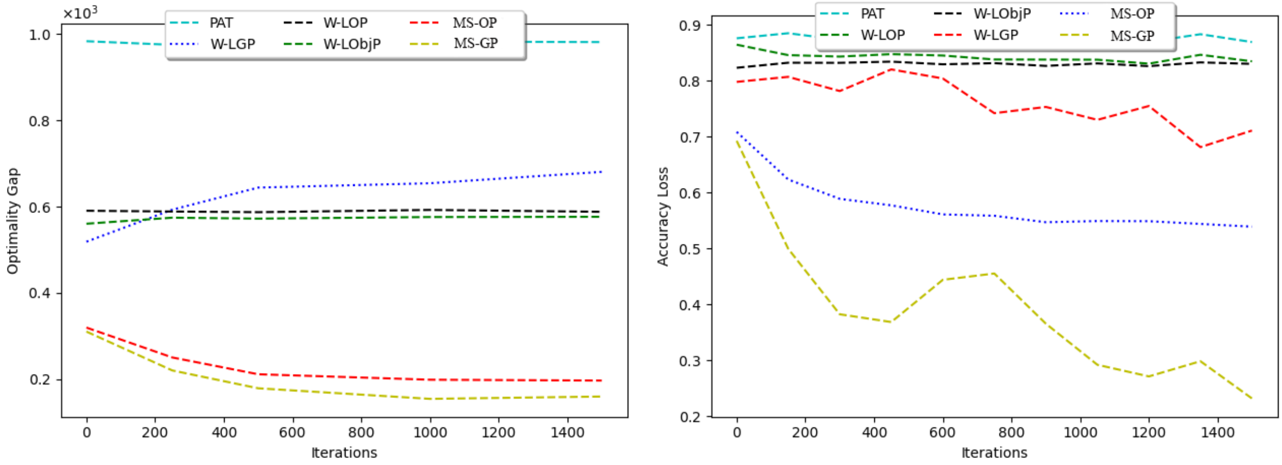

Figure 4. Relative accuracy loss and optimality gap comparison on adult (p = 1000). All models have privacy budget of $\epsilon = 0.05$ for each iteration.)

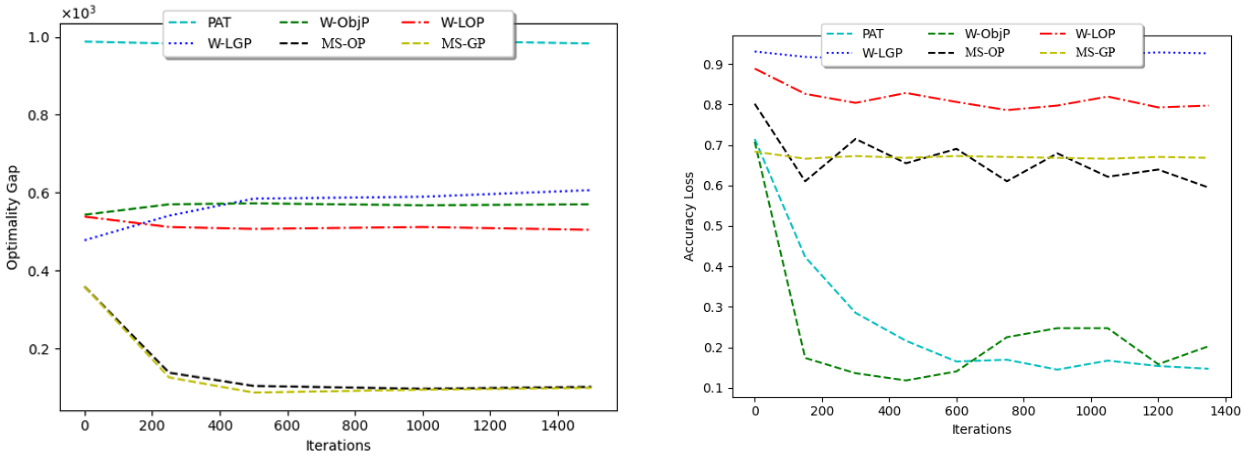

Figure 5. Relative accuracy loss and pptimality gap comparison on CICMalDroid2020 (p = 1000). (Entire models contains privacy budget of $\epsilon = 0.05$ for each iteration.)

Result on Adult Dataset: The Adult [44] data is a composition of demographic information of approximately 47,000 individuals, In this domain, our duty is to predict if annual income of data owners is exceed or below $50,000.00 threshold. During the pre-processing stage, we obtained 104 features for each of the records, whiles the missing values were removed therefore yielding 45,222 records with 30,000 of them now forming the training dataset whiles the rest are used for the testing of our model. In our simulation on the Adult dataset, our proposed MS-OP and MS-GP methods outperform the benchmarks both with respect to the accuracy loss and optimality gab as demonstrated in Figure 4.

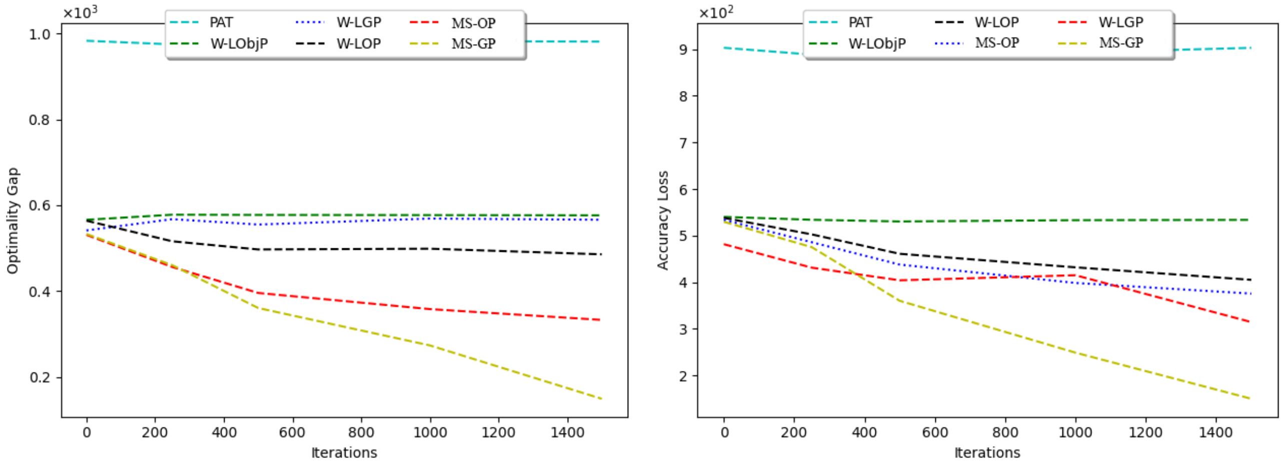

Figure 6. Relative accuracy loss and optimality gap comparison on CICIDS2018 (p = 1000). All models have privacy budget of $\epsilon = 0.05$ for each iteration.)

Result on CICMalDroid2020 Dataset: As the amount of data owners p grows and with the decrease in the size of the local data, the relative accuracy of all the models begins to decrease with the exclusion of MS-GP as represented in Figure 5. It is obvious that the performance of the benchmarks algorithms begins to depreciate basically owing to the huge volumes of statistical noise injected within the classifier. Furthermore, the performance of MS-OP also deteriorates with the reduction in the size of the local dataset owing to the loss in information from partitioning of the dataset which has been one of the challenges with the aggregation of locally trained classifiers.

Result on CICIDS2018 Dataset: With the reduction in the amount of local dataset which is as a result of the decrease in the number of data owners p, there is a great decrease in the performance of all the methods with the exception of MS-GP (Figure 6). Although there is a reduction in the performance of MS-OP as the size of the local dataset is reduced, it continues to outperform the benchmarks of existing model aggregation. We observed that as $p = 1000$, the performance of W-LObjP is weaker as compared to the W-LOP, this is due to the deviation in the objective function of W-LObjP (n). It is important to note that the utility of PAT is greatly affected as a result of the huge amount of statistical noise injected into the model, resulting in the plot been out of range for $p = 1000$ (Figure 6).

Table 3 is a summary of the amount of noise for the individual algorithms requires to preserve differential privacy. As stated in Table 3, MS-GP add the lowest amount of statistical noise to the model. Though it is obvious W-LOP injects noise in a similar range as our proposed MS-GP, it applies the statistical noise in a profoundly different approach. Whereas the existing algorithms inject the sampled statistical noise into the optimal non-private model either thorough output perturbation and gradient perturbation to minimize the objective function $J(\theta)$,whiles optimizing an exclusively different objective function $R'(\theta) = R(\theta) + Lap\left(\frac{2G}{p_1\epsilon}\right)$, therefore explaining the increases in optimality gap as the value for the amount $p_{(1)}$ of the dataset decreases.

Table 3. Noise magnitudes compared with diverse multi-party DP algorithms.

PAT	W-LOP	W-LObjP	W-LGP	MS-OP	MS-GP
$\mathcal{L}$ - Laplace, $\mathcal{N}$- Gaussian					
$\mathcal{L}(\frac{2G}{p_{(1)}\lambda\epsilon})$	$\mathcal{L}(\frac{2G}{\sqrt{m}p_{(1)}\lambda\epsilon})$	$\mathcal{L}(\frac{2G}{p_{(1)}\epsilon})$	$\mathcal{N}(\frac{\sqrt{2T}G}{\sqrt{m}p_{(1)}\epsilon})$	$\mathcal{L}(\frac{2G}{mp_{(1)}\lambda\epsilon})$	$\mathcal{N}(\frac{\sqrt{2T}G}{mp_{(1)}\epsilon})$
m=100, $p_{(1)}$=500, λ=0.01, ϵ=0.5, G=1 and T=100 with the Generated Noise Input					
769×10^{-3}	80.0×10^{-3}	7.98×10^{-3}	5.66×10^{-3}	7.98×10^{-3}	0.46×10^{-3}
Standard deviation over 1000 samples for the generated noise					
1149×10^{-3}	111×10^{-3}	10.99×10^{-3}	4.98×10^{-3}	11.90×10^{-3}	0.591×10^{-3}

Table 4. Simulation results.

Dataset	ϵ	δ	Error		Runtime	
			MS-GP (ϵ, δ)	[13](ϵ, δ)	MS-GP (ϵ, δ)	[13](ϵ, δ)
Adult	0.05	0.001	0.0912	0.3692	10.896	202.12
	0.5		0.0212	0.6082	68.504	253.72
	0.1		0.0429	0.6227	22.814	255.12
CICMalDroid2020	0.05	0.001	0.1714	1.3545	10.214	532.12
	0.5		0.2231	1.4585	36.796	519.33
	0.1		0.3983	2.2552	12.613	518.67
CICIDS2018	0.05	0.001	0.0092	0.3039	11.036	185.32
	0.5		0.0101	0.4162	13.893	190.87
	0.1		0.0292	0.4202	4.977	190.32

Variations in Parameters for the Simulation : It's important to note that all of the real-world datasets we used in the experiments have a variety of numerical and categorical characteristics. We apply some of the most common pre-processing agorithms in machine learning, such as converting all categorical features into a collection of binary variables by creating one binary variable for each individual distinct class; and re-scaling all numerical features into the range of [0,1] to ensure that all features have the same size. To meet the specification, we normalized each observation to a unit norm ($i.e., \| \ x \ \|_2 = 1 \ for \ i = 1, 2, ..., p$). To compare our approach to other standard methods on a real-world data set in order to demonstrate its efficacy.

$$\min_{\mathbf{w}} \frac{1}{n} \sum_{i=1}^{n} \log\left(1 + \exp\left(-y_i \mathbf{w}^{\top} \mathbf{x}_i\right)\right) + \frac{\lambda}{2} \|\mathbf{w}\|_2^2$$

Specifically, we also consider (regularized) logistic regression on the three(3) real world data sets. We therefore validate the minimization error $\mathbb{E}F\left(w_{privacy}, S\right) - F(\hat{w}, S)$ and running time of our algorithms based on different $\epsilon = \{0.05, 0.5, 0.1\}$ and $\delta = 0.001$ (see Table 4 for more details).

6. Conclusions

In this work, we prove that an appreciable among of statistical noise in a distributed learning domain can be reduced when it is generated and injected into a model within a secure multi-party computation. Our paper shows how the statistical noise as a prerequisite for our distributed learning domain may be minimized by generating and injecting noise inside a secure computation. Both of our proposed multi-scheme output perturbation (MS-OP) and gradient perturbation (MS-GP) algorithms were both to achieve ϵ-DP and (δ, ϵ)-differential privacy respectively. Though the aggregation of our locally trained models requires only a single secure aggregation, it still remains very efficient. Our MS-GP method has also been able to improve on the optimization algorithm in this multi-party differential privacy setting whereby the privacy budget at each iteration has been adaptively determined depending on the utility of privacy-preserving statistics. In the future, we will try and explore the potential of our framework in other domains.

Acknowledgement

This work was supported in part by the National Natural Science Foundation of China (No.61672135), the Frontier Science and Technology Innovation Projects of National Key R&D Program (No.2019QY1405), the Sichuan Science and Technology Innovation Platform and Talent Plan (No.20JCQN0256), and the fundamental Research Funds for the Central Universities (No.2672018ZYGX2018J057).

Conflict of interest

All authors declare that there is no conflicts of interest in this paper.

References

1. X. Chen, L. Yu, T. Wang, A. Liu, X. Wu, B. Zhang, et al., Artificial intelligence-empowered path selection: A survey of ant colony optimization for static and mobile sensor networks, *IEEE Access*, **8** (2020), 71497–71511.
2. M. A. R. Ahad, A. D. Antar, M. Ahmed, *IoT Sensor-Based Activity Recognition - Human Activity Recognition*, Intelligent Systems Reference Library, Springer, **173** (2021).
3. J. Lin, G. Srivastava, Y. Zhang, Y. Djenouri, M. Aloqaily, Privacy-preserving multiobjective sanitization model in 6G IoT environments, *IEEE Int. Things J.*, **8** (2021), 5340–5349.
4. C. Iwendi, S. A. Moqurrab, A. Anjum, S. Khan, S. Mohan, G. Srivastava, N-sanitization: A semantic privacy-preserving framework for unstructured medical datasets, *Comput. Commun.*, **161** (2020), 160–171.
5. C. Dwork, F. McSherry, K. Nissim, A. D. Smith, Calibrating noise to sensitivity in private data analysis, *J. Priv. Confidentiality*, **7** (2016), 17–51.
6. J. Du, F. Bian, A privacy-preserving and efficient k-nearest neighbor query and classification scheme based on k-dimensional tree for outsourced data, *IEEE Access*, **8** (2020), 69333–69345.

7. J. Liu, Y. Tian, Y. Zhou, Y. Xiao, N. Ansari, Privacy preserving distributed data mining based on secure multi-party computation, *Comput. Commun.*, **153** (2020), 208–216.

8. C. Gentry, Fully homomorphic encryption using ideal lattices, in *Proceedings of the 41st Annual ACM Symposium on Theory of Computing*, ACM, (2009), 169–178.

9. H. K. Bhuyan, N. K. Kamila, Privacy preserving sub-feature selection in distributed data mining, *Appl. Soft Comput.*, **36** (2015), 552–569.

10. A. Gascón, P. Schoppmann, B. Balle, M. Raykova, J. Doerner, S. Zahur, et al., Privacy-preserving distributed linear regression on high-dimensional data, *PoPETs*, **2017** (2017), 345–364.

11. K. Chaudhuri, C. Monteleoni, A. D. Sarwate, Differentially private empirical risk minimization, *J. Mach. Learn. Res.*, **12** (2011), 1069–1109.

12. M. A. Pathak, S. Rane, B. Raj, Multiparty differential privacy via aggregation of locally trained classifiers, in *NIPS*, (2010), 1876–1884.

13. B. Jayaraman, L. Wang, D. Evans, Q. Gu, Distributed learning without distress: Privacy-preserving empirical risk minimization, *Adv. Neural Inf. Proc. Syst.*, 6346–6357, 2018.

14. L. Tian, B. Jayaraman, Q. Gu, D. Evans, Aggregating private sparse learning models using multi-party computation, in *NIPS Workshop on Private Multi-Party Machine Learning*, 2016.

15. M. Bun, T. Steinke, Concentrated differential privacy: Simplifications, extensions, and lower bounds, in *Theory of Cryptography Conference*, Springer, Berlin, Heidelberg, (2016), 635–658.

16. Y. Chen, Y. Mao, H. Liang, S. Yu, Y. Wei, S. Leng, Data poison detection schemes for distributed machine learning, *IEEE Access*, **8** (2020), 7442–7454.

17. E. Alsuwat, H. Alsuwat, M. Valtorta, C. Farkas, Adversarial data poisoning attacks against the PC learning algorithm, *Int. J. Gen. Syst.*, **49** (2020), 3–31.

18. M. Aliasgari, M. Blanton, F. Bayatbabolghani, Secure computation of hidden markov models and secure floating-point arithmetic in the malicious model, *Int. J. Inf. Sec.*, **16** (2017), 577–601.

19. O. Catrina, A. Saxena, Secure computation with fixed-point numbers, in *International Conference on Financial Cryptography and Data Security*, Springer, Berlin, Heidelberg, (2010), 35–50.

20. A. C. Yao, Protocols for secure computations, in *23rd annual symposium on foundations of computer science (sfcs 1982)*, IEEE, (1982), 160–164.

21. O. Goldreich, Secure multi-party computation, *Manuscr. Prelim. Version*, **78** (1998).

22. I. Damgård, C. Orlandi, Multiparty computation for dishonest majority: From passive to active security at low cost, in *Annual cryptology conference*, Springer, Berlin, Heidelberg, (2010), 558–576.

23. R. Shokri, V. Shmatikov, Privacy-preserving deep learning, in *Proceedings of the 22nd ACM SIGSAC conference on computer and communications security*, (2015), 1310–1321.

24. R. Bendlin, I. Damgård, C. Orlandi, S. Zakarias, Semi-homomorphic Encryption and Multiparty Computation, *Advances in Cryptology - EUROCRYPT 2011 - 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tallinn, Estonia, May 15-19, 2011. Proceedings*

25. J. B. Nielsen, P. S. Nordholt, C. Orlandi, S. S. Burra, A new approach to practical active-secure two-party computation, in *Annual Cryptology Conference*, Springer, Berlin, Heidelberg, (2012), 681–700.

26. A. Bansal, T. Chen, S. Zhong, Privacy preserving back-propagation neural network learning over arbitrarily partitioned data, *Neural Comput. Appl.*, **20** (2011), 143–150.

27. J. Yuan, S. Yu, Privacy preserving back-propagation neural network learning made practical with cloud computing, *IEEE Trans. Parallel Distrib. Syst.*, **25** (2014), 212–221.

28. W. Zhang, A BGN-type multiuser homomorphic encryption scheme, in *2015 International Conference on Intelligent Networking and Collaborative Systems*, IEEE, (2015), 268–271.

29. E. Hesamifard, H. Takabi, M. Ghasemi, C. Jones, Privacy-preserving machine learning in cloud, in *Proceedings of the 2017 on cloud computing security workshop*, (2017), 39–43.

30. P. Li, J. Li, Z. Huang, T. Li, C. Gao, S. Yiu, et al., Multi-key privacy-preserving deep learning in cloud computing, *Future Gener. Comput. Syst.*, **74** (2017), 76–85.

31. P. Mukherjee, D. Wichs, Two round multiparty computation via multi-key FHE, in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Springer, Berlin, Heidelberg, (2016), 735–763.

32. R. Agrawal, R. Srikant, Privacy-preserving data mining, in *Proceedings of the 2000 ACM SIGMOD international conference on Management of data*, (2000), 439–450.

33. P. K. Fong, J. H. Weber-Jahnke, Privacy preserving decision tree learning using unrealized data sets, *IEEE Trans. Knowl. Data Eng.*, **24** (2012), 353–364.

34. J. M. Abowd, The US census bureau adopts differential privacy, in Proceedings of the 24th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, (2018), 2867–2867.

35. F. Liu, Generalized gaussian mechanism for differential privacy, *IEEE Trans. Knowl. Data Eng.*, **31** (2019),747–756.

36. C. Dwork, A. Roth, The algorithmic foundations of differential privacy, *Found. Trends Theor. Comput. Sci.*, **9** (2014), 211–407.

37. C. Dwork, G. N. Rothblum, S. P. Vadhan, Boosting and differential privacy, in *2010 IEEE 51st Annual Symposium on Foundations of Computer Science*, IEEE, (2010), 51–60.

38. O. Kwabena, Z. Qin, T. Zhuang, Z. Qin, Mscryptonet: Multi-scheme privacy-preserving deep learning in cloud computing, *IEEE Access*, **7** (2019), 29344–29354.

39. A. Albarghouthi, J. Hsu, Synthesizing coupling proofs of differential privacy, *Proc. ACM Program. Lang.*, **2** (2017), 1–30.

40. K. Chaudhuri, C. Monteleoni, Privacy-preserving logistic regression, in *NIPS*, **8** (2008), 289–296.

41. J. Zhang, T. He, S. Sra, A. Jadbabaie, Why gradient clipping accelerates training: A theoretical justification for adaptivity, preprint, arXiv: 1905.11881.

42. S. Alipour, F. Mirzaee, An iterative algorithm for solving two dimensional nonlinear stochastic integral equations: A combined successive approximations method with bilinear spline interpolation, *Appl. Math. Comput.*, **371** (2020), 124947.

43. Y. Wang, D. Kifer, J. Lee, Differentially private confidence intervals for empirical risk minimization, *J. Priv. Confidentiality*, **9**, (2019).

44. M. Lichman, *UCI machine learning repository*, 2013. Available from: http://archive. ics. uci. edu/ml.

45. I. Sharafaldin, A. H. Lashkari, A. A. Ghorbani, Toward generating a new intrusion detection dataset and intrusion traffic characterization, in *ICISSp*, (2018), 108–116.

46. S. Mahdavifar, A. F. A. Kadir, R. Fatemi, D. Alhadidi, A. A. Ghorbani, Dynamic android malware category classification using semi-supervised deep learning, in *2020 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech)*, IEEE, (2020), 515–522.

AIMS Press