MSDP: multi-scheme privacy-preserving deep learning via differential privacy

Kwabena Owusu-Agyemeng¹ · Zhen Qin¹ · Hu Xiong¹ · Yao Liu¹ · Tianming Zhuang¹ · Zhiguang Qin¹

Received: 14 June 2020 / Accepted: 25 February 2021 / Published online: 21 March 2021
© The Author(s) 2021

Abstract

Human activity recognition (HAR) generates a massive amount of the dataset from the Internet of Things (IoT) devices, to enable multiple data providers to jointly produce predictive models for medical diagnosis. That the accuracy of the models is greatly improved when trained on a large number of datasets from these data providers on the untrusted cloud server is very significant and raises privacy concerns. With the migration of a deep neural network (DNN) in the learning experience in HAR, we present a privacy-preserving DNN model known as Multi-Scheme Differential Privacy (MSDP) depending on the fusion of Secure Multi-party Computation (SMC) and ϵ -differential privacy, making it very practical since existing proposals are unable to make all the fully homomorphic encryption multi-key which is very impracticable. MSDP inputs a secure multi-party alternative to the ReLU function to reduce the communication and computational cost at a minimal level. With the aid of experimental verification on the four of the most widely used human activity recognition datasets, MSDP demonstrates superior performance with very good generalization performance and is proven to be secure as compared with existing ultramodern models without breach of privacy.

Keywords Internet of Things · Differential privacy · Fully homomorphic encryption · Privacy-preserving secure multi-party computations

1 Introduction

Human activity recognition (HAR) generates massive amounts of data from the synergy of communication [1–3] and the medical Internet of Things [4, 5]. Analysis of HAR datasets is useful since it enhances the health status of patients as experts have demonstrated a clear correlation between overweight, physical activity, cardiac arrest, obesity, and metabolism-related syndromes. However, preserving the privacy of these datasets is a fundamental problem for many real-world applications. To avoid the violation of user's privacy and the exposure of healthcare providers to legal (HIPPA/HITECH law) [6] subpoenas, two major privacy-preserving techniques have been proposed

to control the high risk of leakage to address privacy concerns. The two major algorithms are fully homomorphic encryption [7, 8] and differential privacy [9].

Differential privacy as a data distortion method perturbs the existing raw dataset by the addition of statistical noise or dataset swapping to avoid inferring information about any specific record while retaining the statistical property over the processed datasets. The injection of statistical noise is independent of the magnitude of the data. Consequently, considering a very large dataset, a considerable level of data privacy preservation can be accomplished by the addition of a small amount of noise. Data owners also require careful calibration to balance privacy and model usability. Fully homomorphic encryption [30] has demonstrated more promising solutions towards the protection of privacy of user data. It allows data owners to encrypt their datasets with their individual public keys before outsourcing computations to the cloud service provider. Mathematical computations and training of the models are performed by the cloud server on the encrypted dataset to output ciphertext results. The cloud server cannot access any of the user information at this point since it does not possess the private keys.

✉ Kwabena Owusu-Agyemeng
cooljacko@gmail.com

¹ School of Information and Software Engineering, University of Electronic Science and Technology of China, Chengdu, China

As the size of data and computation increases, Fully Homomorphic Encryption (FHE) [22] has been integrated into deep learning to take advantage of the convenience, flexibility, storage, and higher computational capabilities to process inference queries. On the grounds that DNN has also been increasingly used in various human activity recognition tasks to exhibit excellent levels of performance, obviously, the generalization of the performance of deep neural network models is distinctly stimulated by the value and capacity of the dataset for training the model.

To improve on the training models, collaborative learning has been the preferred choice with the consolidation of multiple datasets which is extremely difficult for an individual data owner to provide.

Motivation Consider the deployment of Industrial Internet of Things (IIoT) [28] or Internet of Medical Things (IoMT) [29] devices by different industry or medical centers. These wearable devices are used to recognize human activities to aid in the production of diagnostic models, with the potential to monitor the health-related behavior of individuals from these encrypted patient datasets.

However, this paper is motivated by three fundamental issues: (i) The black-box properties of the deep neural network have the potential of leading to privacy concerns of applications on data obtained from human activity recognition, i.e., it is very difficult to pre-expect exactly what the networks learn from the datasets, due to result of the optimization; they possibly learn features that could accurately estimate user demographics without any intentional design. This might expose the datasets to the malicious cloud server or unauthorized users, e.g., hackers, which results in the disclosure of the user's confidential data. (ii) The malicious cloud server is untrusted and might render the data vulnerable to attacks during storage and computation. During this time, data owners are unable to control the usage of their private data by the cloud service provider. (iii) With respect to the anticipated malicious behavior of the cloud server, multiple data owners may choose a pre-treat FHE Privacy-Preserving (PP) technology to encrypt individual raw datasets prior to outsourcing the datasets to an untrusted cloud server for computational analysis and data storage. Another interesting issue evolves from whether all the different FHE schemes from the individual data owners can be transformed to multi-key in MK-FHE [24] to aid the data aggregation of the training of the collaborative deep learning model. The construction of a privacy-preserving deep learning model to learn from the aggregated datasets from multiple parties with multiple keys still remains a challenge in both industry and academia.

With the exploitation of the unique potential of differential privacy (DP) and careful examination of existing FHE primitives, we present a collaborative privacy-preservation

scheme over encrypted data from multiple parties with different public keys to address these issues. This paper proposes an innovative paradigm named Multi-Scheme Privacy-preserving DNN learning with differential privacy (MSDP). This is to resolve the outlined issues. The inherent blueprint depends on demonstrating that regardless of the aggregated ciphertext encrypted with multiple encryption keys, the cloud server will be allowed to inject the corresponding different statistical noise based on different queries of the data owner. This proposed scheme differs from existing work where statistical noise is infused by the DP before outsourcing to the cloud server. The presence of the Evaluate algorithm enables the user to generate ciphertext ψ of the required result. In the honest-but-curious model, MSDP architecture expresses the necessary security [10] assurance based on differential privacy and its underlying FHE [22] cryptosystem, i.e., there is a highly negligible chance by hackers to leak the privacy of the dataset since they are globally protected by encryption. MSDP offers a more feasible approach while improving the accuracy and efficiency of the computations.

In the MSDP framework, our assumption depends on data analyst (DA) and computational evaluator (CE) may not collude since both participating entities are curious and semi-honest. During these stages in MSDP primitive, several data providers do not collude with one another. The principal contribution to this work can be summarized threefold as follows:

- In our proposed MSDP, a collaborative privacy-preserving DNN architecture gives the computational evaluator the authority to inject different statistical noise to the offloaded datasets based on the distinct queries from the DA without delegating this task to the data providers. In MSDP, the computational evaluator (cloud server) is not required to choose any type of FHE [22] scheme for data providers before meeting the encryption requirements of the computational evaluator.
- The Multi-Scheme privacy-preserving DNN scheme is capable of aggregating data provider's datasets, preserving the privacy of the confidential datasets, intermediate results, and the learning model. MSDP has greatly improved the accuracy and efficiency of the training model while circumventing the errors that dramatically degrade the accuracy with the introduction of alternative nonlinear ReLU function polynomial approximation and Batch Normalization (BN) without privacy leakages.
- MSDP is validated on a randomized dataset with ϵ -DP rather than on the encrypted dataset to improve the productivity and accuracy of the learning model. Our simulations indicate the practicality and feasibility of our model.

The organization of the rest of the paper is as follows: Section 3 presents some preliminaries and the definition of FHE related to this paper. 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 MSDP, and Section 7 performs the security analysis of our innovative model while Section 8 completes our whole work.

2 Related works

A majority of the existing privacy-preserving methods in DNN are based on Secure Multiparty Computation (SMC) to ensure a possible method for computational privacy. This allows the entity executing the privacy-preserving algorithm to be replaced with multiple entities during the training of the model in the distributed settings, while individual data owners remain oblivious to both the input dataset and the intermediate output. One of the promising alternatives currently is ϵ -DP which has gained considerable research attention for the provision of privacy against adversaries. Since diverse records or columns of a database may contain unrelated confidential data [11], ϵ -DP has been generalized to consider all these properties. Personalized differential privacy [12], therefore, assigns a privacy budget separately to each record in the database, not the entire database which will also improve on the commutation involving data utility and privacy. Output to queries basically may depend predominantly on a subset of entire records, while the budget will be the only record lowered therefore giving additional independence to the data requesters to efficiently formulate their queries. Exploring the synergy between ϵ -DP and SMC on a joint distribution of multiple entities is a significant and difficult challenge [13]. Considering the joint multi-party domain, given n local datasets $\{D_1, D_2, D_3, \dots, D_n\}$ with a function f , computation of a $f(\bigcup_{i=1}^n D_i)$ with the aim of satisfying ϵ -differential privacy on each of the local datasets D is a difficult problem. Based on the SHAREMIND SMC framework [14, 15] Pettai et al. [16] demonstrated the fast method of applying DP with less noise on top of SMC in order to obtain reasonable accuracy and efficiency, while Goryczka et al. [17] also explored the potential of differential privacy and secure multi-party computations to propose an enhanced fault-tolerant scheme to solve the complexities of secured [18] data aggregation in distributed settings. Dataset aggregation is achieved with the aid of their enhanced secured multi-party computations schemes. ϵ -DP of the intermediate results is achieved either by distributed Laplace of geometric mechanism while the approximated ϵ -DP is achieved by diluted mechanism before making the data public. The unprecedented accuracy of machine learning algorithms is also confronted with

privacy concerns. Machine learning (ML) has therefore been turned into privacy-preserving with differential privacy protection. This is to enable hospitals, insurance companies, and other corporate bodies to generate large-scale volumes of data to benefit from this technology due to the successful achievement of ML methods is directly proportional to the amount of dataset accessibly during the learning processes.

3 Preliminaries

In this section, we design our MSDP algorithms by composing a number of existing tools based on the literature, namely NTRU Encryption [23], Multikey Homomorphism [24], Laplace mechanism [25] of Dwork, deep neural network, formal definition, security model and system model as the building blocks used throughout the whole paper. In this paper, we are motivated by FHE from NTRU primitive with modification of NTRUEncrypt.

This unit presents specific notations and FHE schemes applied in our framework in Table 1.

Definition 1 (NTRU Encryption). Let n, q, p, σ, α be the parameters. The parameters n and q define the rings $\mathcal{R}$ and $\mathcal{R}_q$. $p \in \mathcal{R}_q^\times$ defines the plaintext message space as $\mathcal{P} = \mathcal{R}/p\mathcal{R}$. This must be a polynomial with “small” coefficients with respect to q while requiring $\mathcal{N}(p) = |\mathcal{P}| = 2^{\Omega(n)}$ at the same time to enable lot of bits to be encoded at once. Typical choices applied in the schemes are $p = 3$ and $p = x + 2$ but in this scenario since q is prime, we may also choose $p = 2$. By the reduction of the modulo px^i ’s can be written in any element as $\sum_{0 \leq i < n} \epsilon_i x^i p$ with $\epsilon_i \in (-1/2, 1/2)$. Using the fact that $R = \mathbb{Z}[x]/(x^n + 1)$, we therefore assume that any element of $\mathcal{P}$ is an element of $\mathcal{R}$ with the infinity norm $\leq (\deg(p) + 1) \cdot \|p\|$. α is the R-LWE noise distribution parameter. Finally, the parameter σ is the standard deviation of the discrete Guassian distribution used during the key generation process. Given the security parameter k , NTRUEncrypt scheme can be specialized as follows:

Table 1 Notations in our MSDP protocol

Acronym	Description
CE	Computational evaluator
CSP	Crypto service provider
DP	Data provider
DA	Data analyst
(pk_i, sk_i)	Data provider’s public and secret key
(pk_0, sk_0)	Crypto service provider’s public and secret key
$\mathcal{C}$	Classifier
$\mathcal{C}(x, \theta)$	Prediction of $\mathcal{C}$ with input x and θ

- $\text{KeyGen}(1^k)$: The key generation algorithm samples polynomials f' from $\mathcal{D}_{z^n}$, σ ; let $f = p \cdot f' + 1 \pmod{q}$ ($f \pmod{q} \notin \mathcal{R}_q^\times$ then resample g from $\mathcal{D}_{z^n}$; if $(g \pmod{q}) \notin \mathcal{R}_q^\times$, by resampling the secret key and public key will return $sk = f$ and $pk = h = pg/f \in \mathcal{R}_q^\times$
- $\text{Enc}(pk, m)$: Given ciphertext $\mathcal{M} \in \mathcal{P}$, set $s, e \leftarrow \mathcal{R}_\alpha$ and return ciphertext $\mathcal{C} = hs + pe + \mathcal{M} \in \mathcal{R}_q$
- $\text{Dec}(sk, c)$: Given ciphertext $\mathcal{C}$ and secret key f , compute $\mathcal{C}' = f \cdot \mathcal{C} \in \mathcal{R}_q$ and return $\mathcal{C}' \pmod{p}$

3.1 MS-FHE in MSDP architecture

The Multi-Key Fully Homomorphic Encryption (MK-FHE) [24, 26, 27] scheme in MSDP comprises six algorithms: KeyGen, Enc, Dec, Eval, uDecrypt and uEvaluate. These primitives are basically well-defined as follows:

- $\text{KeyGen}(1^k)$: For a security parameter k , outputs a public key pk , a private key sk , and a (public) evaluation key ek .
- $\text{Enc}(pk, m)$: Given a public key pk and a message m , outputs a ciphertext c .
- $\text{Dec}(sk, c)$: Given a private key sk and a ciphertext c , outputs a message m .
- $\text{Eval}(ek, \mathcal{C}, c_1, \dots, c_l)$: Given an evaluation key ek , a (description of a) circuit $\mathcal{C}$ and l ciphertexts $c_1, \dots, c_l$, outputs a ciphertext c .
- Decrypt : It is a deterministic scheme when input a ciphertext ψ and scheme-key pairs (s_i, sk_i) , outputs a plaintext: $x \leftarrow \text{Decrypt}(\langle s_1, sk_1 \rangle, \dots, \langle s_t, sk_t \rangle, \psi)$, where s_i indicates scheme $\mathcal{E}^{(si)}$ and sk_i is a secret key generated by $\text{KeyGen}^{(si)}$
- uEvaluate : It takes the circuit $\mathcal{C}$ as input, a number of 3-tuples $\langle s_i, pk_i, \psi_i \rangle$, $1 \leq i \leq t$, where s_i is an index indicating scheme $\mathcal{E}^{si}$, pk_i is a public key generated by KeyGen^{si} and ψ_i is a ciphertext under encryption key pk_i and scheme $\mathcal{E}^{si}$, i.e., $\psi_i \leftarrow \text{Enc}^{(si)}(pk_i, x_i)$ for some plaintext x_i . The output of uEvaluate is a ciphertext: $\psi := \text{uEvaluate}(\mathcal{C}, \langle s_1, pk_1, \psi_1 \rangle, \dots, \langle s_t, pk_t, \psi_t \rangle)$.

3.2 Dynamic ϵ -differential privacy

Let us recollect the basic description of ϵ -differential privacy.

Definition 2 (ϵ -DP). A randomized mechanism $f : D \rightarrow \mathcal{R}$ satisfies ϵ -differential privacy (ϵ -DP) if for any adjacent $D, D' \in \mathcal{D}$ and $S \subset \mathcal{R}$

$$\Pr[f(D) \in S] \leq e^\epsilon \Pr[f(D') \in S] \quad (1)$$

where the probability $\Pr[\cdot]$ is taken over the randomness of mechanism f and also shows the risk of privacy disclosure.

The definition above is contingent on the notion of adjacent input D and D' which is domain-specific and it is typically chosen to capture the contribution to the mechanism's input by a single individual. ϵ is a predefined privacy parameter for controlling the privacy budget; the smaller ϵ the stronger the privacy protection. The formal definition of sensitivity is given below (Definition 3).

Definition 3 (Sensitivity) Assume f is a numeric query function that maps a datasets D into a d -dimensional real space $\mathbb{R}^d$, i.e., $f : D \leftarrow \mathbb{R}^d$. For a pair of neighboring datasets D and D' , the sensitivity f is defined as:

$$\Delta f = \frac{\max}{D, D'} \|f(D) - f(D')\|_{L_1} \quad (2)$$

where $\|\cdot\|_{L_1}$ denotes the L_1 norm.

Theorem 1 (Laplace mechanism) The Laplace mechanism is a prototypical ϵ -differentially private algorithm, therefore allowing the release of an approximate to an arbitrary query with values in $\mathbb{R}^d$. Let $\sigma \in \mathbb{R}^+$, and f is a numeric query function that maps a domain D into d -dimensional real space $\mathbb{R}^d$, i.e., $f : D \leftarrow \mathbb{R}^d$. The computation $\mathcal{M}$

$$\mathcal{M}(x) = \{x\} + (\text{Lap}_1(\sigma), \text{Lap}_2(\sigma), \dots, \text{Lap}_d(\sigma)) \quad (3)$$

provides ϵ -differential privacy, where the noise $\text{Lap}_1(\sigma)(i \in [1, d])$ is drawn from the Laplace distribution with scaling parameter σ , whose density function is:

$$p(\sigma) = \frac{1}{2\sigma} \exp(-|x|/\sigma) \quad (4)$$

At this point, the parameter $\sigma = \Delta f/\epsilon$ is controlled by the privacy budget ϵ and the function's sensitivity Δf

3.3 System model

MSDP scheme is a composition of four different parties, involving groups of data providers (DP), computational evaluator (CE), data analyst (DA) (i.e., individual data owners), and crypto service provider (CSP). More specifically, respective parties in this system are explained in Fig. 1.

- **DP**: In this setting the assumption is DP contains n DP, denoted by $\{P_1, P_2, P_n\}$, each DP $P_i \in DP$ is a cloud user who keeps dataset $D_i = \left\{ \left(x_j^i, y_j^i \right) \right\} \in X \times Y : j \in [1, p_i], i \in [1, n]$ with data records $r_i = \text{pub}(r) \parallel \text{sec}(r)$, which is the concatenation of public fields $\text{pub}(r)$ and secret field which is denoted as $\text{sec}(r)$. Each of the $D_i (i \in [1, n])$ is of size p_i with data

Fig. 1 System model

vector $x_j^i \in \mathbb{R}$, and the corresponding binary label $y_j^i \in Y := \{0, 1\}$. To protect the privacy of the dataset, each of the DP $P_i \in DP$ independently generating a pair of public and private keys $(pk_i, sk_i) \leftarrow keyGen(1^\lambda)$. They then encrypt their sensitive fields generating a ciphertext: $c_i = pubr_i || Enc(pk_i, sec(r_i))$.

- **CE:** CE is honest-but-curious and holds the data center, it provides the aggregated database by constructing the encrypted database $Enc(\mathcal{X})$, which is a composition of the public key and ciphertext tuples $\langle pk_i, c_i \rangle$ from each data provider. CE combines Laplace noise η_i to the encrypted data for individual DP. The noised-added encrypted dataset can be computed by $Enc(pk_i, \hat{c}_i) \otimes Enc(pk_i, \eta_i)$. The noised-added dataset encrypted with diverse public keys is then published by the CE.
- **CSP:** The CSP simply offers online cryptographic assistances to client. For instance, CSP can manage encrypted and decrypted ciphertext transmitted by CE.
- **DA:** The DA are most of the time individual clients to the cloud service provider and they are capable of gathering feature vectors of their records. In situations where DA queries the CE for secure predictive services, DP then encrypts the queries proceeded by outsourcing to the CE.
- **Malicious adversaries:** In this setting, adversaries are not counted among participants in MSDP architecture. They rather exist since we want to consider the confidentiality of our architecture. This work is basically interested in any malicious adversaries capable of corrupting any subsection of $t > N$ entities as considered. During the process of analyzing the privacy of MSDP, our assumption is based on adversaries possessing strong fundamental knowledge

The interactive scenario between the entities and components is illustrated in Fig. 1.

3.4 Problem statement

In this setting, we assume that the set of DP comprises n DP, expressed as $\{P_1, P_2, P_n\}$, each DP $P_i \in DP$ is a cloud client keeping dataset $D_i = \left\{ \left(x_j^i, y_j^i \right) \right\} \in X \times Y : j \in [1, p_i], i \in [1, n]$ with data records $r_i = pub(r) || sec(r)$, concatenation of public fields $pub(r)$ with corresponding private fields which is denoted as $sec(r)$. Each of the $D_i (i \in [1, n])$ comprises p_i with dataset vector $x_j^i \in \mathbb{R}$, and resultant binary label $y_j^i \in Y := \{0, 1\}$. Owing to the confidential concerns, each DP $P_i \in DP$ independently generating pairs of public and private keys $(pk_i, sk_i) \leftarrow keyGen(1^\lambda)$ to encrypt individual local data prior to outsourcing to CE for data storage and mathematical computations. On these premises, ciphertext under diverse schemes or public keys, CE produces a synthetic data, whereby distinctive statistical noises are added based on dissimilar applications. We therefore discharge the synthetic dataset with ϵ -DP to perform a PP DNN model on our synthetic datasets.

As an MSDP example, we study the problems below:

- Towards overcoming key management budget reduction, DP $\{P_1, P_2, \dots, P_n\}$ should be capable of generating their own pk and sk keys without interacting with DA.
- Furthermore, sustaining computations over encrypted space, CE constructs an aggregated encrypted database $\{Enc(\mathcal{X}) \triangleq \{ \langle pk_i, c_i \rangle \} \}$ and these encryption schemes from DP should possess the characteristics of some malleability and homomorphism.

3.5 Threat model

Assumption in MSDP is that entities involved in the privacy-preserving multi-party process data providers $P_i \in DP(i \in [1, n])$, data analyst, computational evaluator, and cryptographic service providers are non-colluding (i.e., curious-but-honest) adversaries rigorously following our algorithm. On the other hand, their interest is in learning or gathering confidential information throughout the training of the privacy-preserving model. Based on this security assumption, our scheme presents an active malicious adversary A_d in the learning model. The main aim of A_d is to try decrypting the challenge DP's original encrypted data and the challenge CE's encrypted model parameters with the resulting potential:

- i A_d may eavesdrop entire interactions between DP and CE to gain access to the ciphertext to unleash an active attack to tamper, intercept, and forge the transferred messages.
- ii A_d may compromise CE to presume the value of the plaintext of the entire ciphertexts offloaded from DPs, and the whole ciphertexts driven from CSP by implementing the training processes.
- iii A_d may corrupt some DP in generating plaintext data of another ciphertext from other DPs
- iv A_d may compromise an individual or multiple DPs, with the exemption of attacking DPs, gaining access to individual decryption potentials, to guess entire ciphertexts belonging to the DP attack.

Conversely, A_d is therefore prevented from compromising: (i) both CE and CSP concurrently, (ii) the challenge DPs. We state that such constraints are normal in the cryptographic protocol.

3.6 Design goals

As a PP collaborative deep learning model, MSDP enables CE to train and construct models over collaborative DPs while responding to data analyst predictive queries. MSDP should meet the following requirement to resolve the adversary and security model:

- *Classifier accuracy*: MSDP should be capable of classifying correctly for every query from the data analyst while making accurate predictions with high probabilities.
- *Privacy-preserving*: Provision of privacy guarantee by the system should be assured without disclosing confidential information about DP's and classifiers. To achieve our security target, the learning and prediction

stage should remain constructed in ciphertext settings. The data analyst is the only one who will be capable of obtaining the decrypted intermediate results by the application of the private key after the CE has responded to a predictive query. The CSP is not revealed therefore making it hidden to DP.

- *Flexibility*: During MSDP, the CSP is not a static service provider. In this domain, the CSP can be different entities or institutions publishing their corresponding different schemes or different public keys based on different functions or motivations.

4 Proposed MSDP architecture

MSDP architecture focuses on the training of a classification model over aggregated datasets from multiple DP with the aim of offering confidential prediction services for DA with this classification model. In this instance, a set of n mutually non-colluding DPs $\{P_1, P_2, \dots, P_n\}$ outsourced their encrypted data to the CE for storage while allowing it to perform some computational operations on these concatenated datasets. In other to promote the processing over encrypted dataset through possibly diverse fully homomorphic encryption schemes or with even dissimilar public keys, the Multi-Scheme FHE algorithm will contribute to our PP technique while concatenating encrypted datasets from DP prior to offloading to CE. The application of offloaded concatenated ciphertext enables the CE to construct a classification model while storing and maintaining the model in an encrypted form. The classification model in the CE is therefore ready to respond to queries from DP.

4.1 MSDP overview

This section gives a description of the MSDP scheme as a solution to the problem formulated in Section 4. We outline a comprehensive construction of MSDP and demonstrate procedures to achieve secure offloading of data and classification in a secure environment.

- *Secure dataset offloading*. DP encrypts their individual datasets with their preferred choice of Fully Homomorphic encryption primitive to enable them to securely outsource their dataset to the computational evaluator. Each DP individually produces a pair of public/secret keys coupled with the $keyGen(1^\lambda)$ to outsource encrypted dataset under individual public keys to CE. During this domain, the algorithm for the aggregated private data computation depends on ϵ^i which is

capable of concatenating all the dissimilar public keys into ciphertext under the same public key.

- *Noise adding.* At this stage, based on the differential application of queries from the data analyst, the computational evaluator CE adds differential Laplace statistical noise to the offloaded ciphertext. Laplace statistical noise then encrypted under related outsourced constructed database $Enc(\mathcal{X})$
- *Deep learning-based ϵ -DP.* The DA is capable of learning the DNN model with ϵ^i -DP on the noise-added encrypted dataset.

4.2 MSDP detail design

This subsection offers a comprehensive narrative of the MSDP algorithm basically dividing it into three stages: PP training classifiers, generating PP prediction query from DA, PP intermediate results. The general construction of MSDP is shown in Algorithm 3.

4.2.1 Data outsourcing

In this subsection, we discuss our proposed MSDP model. The main work is directed towards the training of classifiers over encrypted settings with data contributed from multiple DP $\{D_1, D_2, \dots, D_n\}$. In this scenario, all parties are encrypting their data with a different fully homomorphic encryption scheme. For a lucid discussion, initially, a setup process for all the schemes is independently initialized and distribute the system confidential parameters. Furthermore, during this stage, depending on diverse motivations or objectives may determine CSP elements with their special functions. Therefore, as soon as the CSP is established, it then distributes private or public key pairs $\{sk_i, pk_i\}$. In this process, each of the data providers individually generates pairs of public and secret keys $pk_i, sk_i \leftarrow KeyGen(1^\lambda)$. Then, they encrypt their secret fields to generate cipher: $r_i = pub(r_i) || Enc(pk_i sec(r_i))$. All DP outsourced their encrypted data ψ_i , along with encryption key pk_i to CE.

4.2.2 Addition of noise

After outsourcing the datasets, the CE therefore generates noise $\{\eta^i = (\eta_1^i, \eta_2^i, \dots, \eta_n^i)\}$ for each of the DP $P_i \in DP$. CE constructs an aggregated encrypted noised database $Enc(\mathcal{X}')$. At this stage, DA can download the noise-added aggregated ciphertext which is now in the form $Enc(\mathcal{X}')$. The data analyst can therefore perform any computation for an n-input function $\mathcal{C}$ on the aggregated noise database as specified in Section 5.

4.2.3 Deep learning-based ϵ -differential privacy

On one occasion, the transformed query results will be computed, and CE sends it back to the DP. As the data provider obtains the encrypted query, the ciphertext ψ_i decrypts to $\mathcal{C}(\mathcal{X})$ with $Decrypt(sk_1, \dots, sk_n; \psi) = \mathcal{C}(X)$ look.

4.3 Polynomial approximation of ReLU

Our proposed model MSDP for a PP classification on DNN has three major requirements: data privacy, the efficiency with reasonably low multiplicative intensity, and higher precision closer to the ultramodern convolutional neural network (CNN). The ReLU function and max pooling functions with high multiplicative depth in the CNN architecture are incompatible with the efficiency requirement of MSDP. At this stage, we modify the CNN model to replace the layers with higher multiplicative intensity, i.e., max pooling and ReLU with lower multiplicative intensity polynomial layers into the CNN model, with a reduction in degradation of the accuracy of the classification. Our aim is to approximate the ReLU function. We, therefore, focus on approximating the ReLU function derivatives instead approximating the rectified linear unit function. The derivative of the activation function is a non-differentiable function similar to a step function at point 0. In situations where the function is the non-infinitely or continuously differentiable function, we thereby approximate it to an appreciable accuracy. We therefore perform an experiment on the derivative of the rectified linear unit function. The sigmoid activation function is an infinitely differentiable, bounded, and continuous function. The structure is similar to the derivative of the rectified linear unit in the large intervals. Furthermore, the sigmoid function is approximated with the polynomials by finding the integral of the polynomial and using it as the activation function. To achieve our goal, we integrate the polynomial approximation of the ReLU plus BN while substituting max pooling by the sum pooling possessing a null multiplicative depth. Furthermore, each ReLU layer is added to the BN layer to enforce a restrictive stable distribution during the entry of the ReLU. The BN layers are therefore added to the training and the classification stage to circumvent high accuracy degradation involving the training stage and classification stage with respect to numerous alterations to the CNN model as described in Table 2, Fig. 2, and Algorithm 1.

After outsourcing the datasets, the CE therefore generates noise $\{\eta^i = (\eta_1^i, \eta_2^i, \dots, \eta_n^i)\}$ for each of the DP $P_i \in DP$. CE constructs an aggregated encrypted noised

Table 2 Polynomial approximation of ReLU

Degree	Polynomials
2	$0.1992 + 0.5002X + 0.1997X^2$
3	$0.1995 + 0.5002X + 0.1994X^2 - 0.0164X^3$
4	$0.1500 + 0.5012X + 0.2981^2 - 0.0004X^3 - 0.0388X^4$
5	$0.1488 + 0.4993X + 0.3007X^2 + 0.0003^3 - 0.0168^4$
6	$0.1249 + 0.5000X + 0.3729X^2 - 0.0410X^4 + 0.0016X^6$

database $Enc(\mathcal{X}')$. At this stage, DA can download the noise-added aggregated ciphertext which is now in the form $Enc(\mathcal{X}')$. The data analyst can therefore perform any computation for an n -input function $\mathcal{C}$ on the aggregated noise-database as specified in Section 5.

4.3.1 Deep learning-based ϵ -differential privacy

On one occasion, the transformed query results will be computed, and CE sends it back to the DP. As the data provider obtains the encrypted query, the ciphertext ψ_i decrypts to $\mathcal{C}(\mathcal{X})$ with $Decrypt(sk_1, \dots, sk_n; \psi) = \mathcal{C}(X)$ look.

Algorithm 1 Batch normalizing transformation.

Input: Values of x over a mini-batch: $\mathcal{B} = \{x_1, \dots, m\}$;
Parameters to be learned: γ, β
Output: $\{y_i = BN_{\gamma, \beta}(x_i)\}$

$$\mu_{\beta} \leftarrow \frac{1}{m} \sum_{i=1}^m x_i \text{ // mini-batch mean}$$

$$\sigma_{\beta}^2 \leftarrow \frac{1}{m} \sum_{i=1}^m (x_i - \mu_{\beta})^2 \text{ // mini-batch variance}$$

$$\hat{x} \leftarrow \frac{(x_i - \mu_{\beta})}{\sqrt{\sigma_{\beta}^2 + \epsilon}} \text{ // normalize}$$

$$y_i \leftarrow \gamma \hat{x}_i + \beta \equiv BN_{\gamma, \beta}(x_i) \text{ // scale and shift}$$
Fig. 2 Approximation of Rectified Linear Unit Function

Our proposed MSDP proposed scheme is a composition of privacy-preserved feedforward propagation (Algorithm 2) and backpropagation (Algorithm 3) with the specifics in Algorithm 3.

Algorithm 2 Privacy-preserved forward propagation.

Input: $\{\psi_1, \psi_2, \dots, \psi_n\} = Enc(\mathcal{X}) \phi = \{W^1, W^2, b^1, b^2\}$;
Output: $z^2, z^3; a^2, a^3$

```

1 for  $i = 1, 2, \dots, i_{max}$  do
2   for  $i = 1, 2, \dots, (n-1)$  do
3     Compute;
4      $z_{j_1 j_2 \dots j_n}^{(2)} = W_{\alpha}^{(1)} \cdot X + b_{j_1 j_2 \dots j_n}^{(1)}$ ;
5      $a_{j_1 j_2 \dots j_n}^{(2)} = f(z_{j_1 j_2 \dots j_n}^{(2)})$ ;
6      $z_{i_1 i_2 \dots i_n}^{(3)} = W_{\beta}^{(2)} \cdot a_{j_1 j_2 \dots j_n}^{(2)} + b_{i_1 i_2 \dots i_n}^{(2)}$ ;
7      $h_{(i_1 i_2 \dots i_n)W, b(X)} = a_{i_1 i_2 \dots i_n}^{(3)} = f(z_{i_1 i_2 \dots i_n}^{(3)})$ ;
8   call Algorithm 3 for backpropagation

```

Algorithm 3 Privacy-preserved backpropagation.

Input : $(\mathcal{X}) \{W^1, W^2, b^1, b^2\}; z^2, z^3; a^2, a^3; \eta$
Output: $\phi = \{W^1, W^2, b^1, b^2\}$

```

1 for  $i = 1, 2, \dots, i_{max}$  do
2   for  $example = 1, 2, \dots, N$  do
3     for  $i_n = 1, 2, \dots, I_1 \times \dots, I_N$  do
4       Calculate;
5        $\sigma_i^{(3)} = (a_i^{(3)} \cdot (1 - a_i^{(3)})) \cdot$ 
 $\sum_{j=1}^{I_1 \times I_2 \times \dots \times I_N} g_{ij} (a_j^{(3)} - y_j) \sigma_{j_1 j_2 \dots j_n}^{(2)} =$ 
 $\left( \sum_{i_1=1}^{I_1} \dots \sum_{i_n=1}^{I_n} w_{\lambda j_1 j_2 \dots j_n}^{(2)} \cdot \sigma_{i_1 i_2 \dots i_n}^{(3)} \right) f'(z_{j_1 j_2 \dots j_n}^{(2)})$ ;
 $i_n = 1, 2, \dots, I_N$ 
 $\Delta b_{i_1 i_2 \dots i_n}^{(2)} = \Delta b_{i_1 i_2 \dots i_n}^{(2)} + \sigma_{i_1 i_2 \dots i_n}^{(3)}$ 
 $\Delta w_{i_1 i_2 \dots i_n j_1 j_2 \dots j_n}^{(2)} =$ 
 $\Delta w_{i_1 i_2 \dots i_n j_1 j_2 \dots j_n}^{(2)} + a_{j_1 j_2 \dots j_n}^{(2)} \cdot \sigma_{i_1 i_2 \dots i_n}^{(3)}$ 
 $b_{j_1 j_2 \dots j_n}^{(1)} = \Delta b_{j_1 j_2 \dots j_n}^{(1)} + \sigma_{j_1 j_2 \dots j_n}^{(2)}$ 
 $\Delta w_{j_1 j_2 \dots j_n i_1 i_2 \dots i_n}^{(1)} =$ 
 $\Delta w_{j_1 j_2 \dots j_n i_1 i_2 \dots i_n}^{(1)} + x_{i_1 i_2 \dots i_n} \cdot \sigma_{j_1 j_2 \dots j_n}^{(2)}$ 
6    $W = W - \eta \cdot \left( \frac{1}{N} \Delta w \right)$ ;
7    $b = b - \eta \cdot \left( \frac{1}{N} \Delta b \right)$ ;

```


Algorithm 4 Overall scheme of MSDP.

Input: $\{m_1, m_2, \dots, m_n\}, \{W^1, W^2, b^1, b^2\};$
 $iteration_{max}$ learning rate η
Output: $\phi = \{W^1, W^2, b^1, b^2\}$

- 1 Data Provider P_i ($i \in [1, k]$) does;
- 2 Initialize the Models parameters randomly;
- 3 Sample a key tuple: $(pk_i, sk_i, ek_i) \leftarrow KeyGen(1^k)$;
- 4 Encrypt private data objects: m_i $W_i^{(j)}$
 $\psi_i \leftarrow pub(m_i) || Enc(pk_i, sec(m_i))$ $d_i \leftarrow$
 $Enc(pk_i, W_i^{(j)})$, $g \leftarrow Enc(pk_i, t_i)$;
- 5 Crowdsourcing the private data to Data Service
 Provider: $(pk_i, ek_i, \psi_i, d_i, g_i)$;
- 6 Computational Evaluator: $Enc(\mathcal{X}) \triangleq \{\langle pk_i, \psi_i \rangle\}$ an
 encrypted database which is the aggregation of public
 keys and ciphertext tuples.;
- 7 Computational Evaluator: Add Laplace noise η_i to
 $Enc(\mathcal{X}, \hat{D}) \triangleq \{\langle pk_i, \psi_i \rangle, \hat{D}\} \otimes \{\langle pk_i, \psi_i \rangle, \eta_i\}$
 Execute *Algorithm 2* and *3* over the ciphertext domain;
- 8 Update the encrypted parameters: $\phi =$
 $\{W^1, W^2, b^1, b^2\}$;;
- 9 Send the learning results γ^* to the Data providers;;
- 10 The Data providers $P_1, P_2, \dots, P_k$ do;;
- 11 The Data providers $P_i, P_2, \dots, P_k$ mutually run a secure
 multiparty protocols to calculate ;
- 12 Evaluate $(C, \{\langle pk_i, \psi_i \rangle, \hat{D}\})$

5 Simulation results

In this segment, we provided experimental outcomes of the MSDP algorithm on data from multiple data owners in the cloud while evaluating the presented algorithm with respect to aggregated encryption time, the cost of deep neural network computation, and the accuracy of our classification model.

5.1 Datasets

In this work, training and testing data are chosen from four benchmark datasets encrypted and outsourced to the cloud representing the typical drawbacks of human activity recognition.

SBHARPT SBHARPT is available publicly online. HAR signals are generated by cellphones with integrated triaxial gyroscope and accelerometer. These devices are attached to the waist possessing a constant frequency rate of 50 Hz to collect 12 different types of activity signals such as walking downstairs, standing and laying, walking upstairs, sitting, and 6 potential activity evolutions: stand-sit, lie-sit, sit-lie,

sit-stand, lie-stand, and stand-lie. This database contains 815,614 proceedings of data from sensors.

Opportunity Dataset from the Opportunity activity recognition is a composition of atomic activities generated with a sensor-based environment in excess of 27,000. The Opportunity dataset comprises recordings of 12 subjects with the application of 15 interconnected sensors along 72 sensors with 10 modalities, incorporated into the WBAN attached to the human body. In this experiment, we consider the sensors on the body, which include initial measurement units and a 3-axis accelerometer. Each of the sensor channels is therefore managed as an individual channel with a whole channel of 113. Opportunity dataset captures different postures and gestures while ignoring the null class. It is a composition of an 18-class classification challenge

PAMAP2 PAMAP2 is human physical activity data generated from 18 activities such as cycling, rope jump, Nordic walk, dancing, lie, sit, stand, run, vacuum clean, iron, ascend and descend stairs, playing soccer recorded from 9 participants (1 female and 8 males), in addition to a variety of leisure activities such as computer work, watch TV, drive a car, clean house, and fold laundry. The gyroscope, accelerometer, magnetometer, and heart rate datasets were recorded via 9 subjects wearing 3 IMU with the aid of a heart rate monitor. The 3 caliber wireless IMU with a selected frequency of 100 Hz: on the dominant arm 1 IMU is placed on the wrist and on the chest respectively, while 1 IMU is also on the dominant side of the ankle. The human recognition monitor with a sampled frequency of 9 Hz is therefore used to monitor the system over 10 h.

Smartphone Smartphone dataset as public dataset is recorded with a waist-mounted cell phone with inertial sensors embedded in the component to collect 30 subjects of activities of daily living (ADL). Thirty volunteers between the ages of 19–48 years were employed in this experiment. Each of the volunteers was engaged in six activities, i.e., walking-upstairs, walking, walking-to-downstairs, standing, sitting, and laying while recording with a Samsung Galaxy S II on their waist. With the aid of the inserted gyroscope and accelerometer, 3-axial angular velocity and 3-axial linear acceleration were captured at a constant rate of 50 Hz. In order to manually label the dataset, the investigations were recorded with a video camera. The dataset was arbitrarily segregated into 70% as learning data and 30% as test data respectively. Noise filters are applied on the accelerometer and gyroscope for the pre-processing while sampling them in a static-width sliding window of 50% overlap and 2.56 s for 128 readings/window. The signals from the accelerometer and gyroscope possess body and

gravitational motion devices which stayed disjointed with butter worth limited-pass screened hooked onto gravity and the accelerated body. The assumption is that gravitational force possesses only limited frequency components, leading to the application of filters with 0.3-Hz termination frequency. In each window, features in the form of vectors were obtained with the calculation of variables from the frequency and time settings grounded on proposed and comparative techniques.

6 Comparison evaluation

This section demonstrates how the MSDP algorithm can protect the data privacy based on MS-FHE cryptosystem and ϵ -differential privacy for deep learning by the addition of noise statistically to the aggregated input. Note that all experiments were carried out on iMac with the specification of 3.4 GHz Intel Core i5, NVIDIA GeForce GTX 780M 4096 MB, and 16 GB 1600 MHz DDR3 RAM. The datasets for this experiment are available public HAR data from PAMAP2, Smartphone, Opportunity, and SBHART datasets. The aggregated samples of datasets are randomly partitioned into 70% of training, 20% validation with 10% testing. We trained a series of different binary classifiers with MSDP based on the four aggregated datasets from HAR. The learning parameters in our experiments are set to $iteration_{max} = 200$, while $\eta = 0.01$.

Accuracy The accuracy loss in MSDP algorithm is analyzed; we performed our classification based on the parameters in our proposed MSDP algorithm and compared it with the non-privacy preserving neural network model.

Table 3 shows the average classification accuracy of the MSDP model and the conventional deep learning computational model which is a non-privacy preserving model. Our algorithm attains promising accuracy as compared to the conventional non-privacy-preserving DNN computational model as exhibited in Fig. 2. The effectiveness of our training model on clean and sanitized datasets is shown in Fig. 3, while the comparison of MSDP with existing models in the HAR public datasets is also demonstrated in Fig. 4.

Table 3 Comparing classification accuracy with state-of-the-art

Models	SBHARPT	PAMAP2	Opportunity
[19]	0.863	0.87	0.84
[20]	0.915	0.906	0.901
[21]	0.920	0.916	0.922
MSDP	0.954	0.935	0.955

Fig. 3 Comparing the accuracy on clean and sanitized datasets

7 Security analysis

This unit basically demonstrates the security evaluation of our fundamental cryptographic encryption schemes with Dynamic ϵ -DP then leading to analyzing the security of the MSDP algorithm.

7.1 Analyzing our encryption algorithm

In the subsequent narratives, we present security proof of the privacy parameter for both our proposed scheme and the security proof of our classifiers. We, therefore, provide a definition of *semantic security*, also well-known as IND-CPA security.

Definition 4 (IND-CPA): Let $\epsilon = (KeyGen, Enc, Eval, Dec, uEvaluate, uDecrypt)$ be a Multi-Scheme Fully homomorphic Encryption scheme and if for any stateful PPT adversary let $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$. For $1^\lambda \in \mathbb{R}$ let

$$\begin{aligned}
 Adv_{\epsilon, \mathcal{A}}^{(IND-CPA)}(1^\lambda) &:= 2Pr[(pk, sk) \leftarrow KeyGen(1^\lambda)]; \\
 (a_0, a_1, state) &\leftarrow \mathcal{A}_1^{O_1}(pk); \\
 b &\leftarrow 0, 1; y \leftarrow Enc(pk, a_b); \\
 \mathcal{A}_2^{O_2}(pk, a_0, a_1, state, y) &= b] \leq \frac{1}{2} + negl(\lambda);
 \end{aligned}$$

where $O_1(\cdot)$ and $O_2(\cdot)$ are evaluation oracles while “state” is secret information using the public key pk . The adversary $\mathcal{A}_1$ output two plaintext a_0, a_1 possesses equivalent dimension $|a_0| = |a_1|$ and padding messages capable of being applied otherwise. We therefore state the

Fig. 4 Performance comparison of MSDP with state-of-the-art models on public datasets

cryptosystem ϵ is IND-CPA secure if $Adv_{\epsilon, A}^{IND-CPA}(1^\lambda)$ and only if the probability that any $\mathcal{A}$ given $\mathcal{C}$, is unable to determine which one is the original message, i.e., there exists a negligible function $negl$ of security parameter λ .

In the one-time encryption (OTE), we present the formal definition as follows:

Definition 5

$$\begin{aligned}
 Adv_{SE, A}^{(OTE)}(1^\lambda) &:= 2Pr[(\lambda) \leftarrow \{0, 1\}; \\
 &\quad (a_0, a_1, state) \leftarrow \mathcal{A}_1(.); \\
 &\quad b \leftarrow 0, 1; y \leftarrow Enc(pk, a_b) : \\
 \mathcal{A}_2(pk, a_0, a_1, state, y) = b] &\leq \frac{1}{2} + negl(\lambda);
 \end{aligned}$$

where a_0 and a_1 are the output of the adversary ∞ possessing equivalent length. We can therefore state that a symmetric encryption $SE=(Enc, Dec)$ is OTE secure if $Adv_{SE}^{(OTE)}$ is negligible.

Data privacy The concatenation $Enc(\mathcal{X})$ of all individual data from data providers is to ensure security and privacy and also promote secure multi-party computation. Based on the previous assertion, we define semantic security.

Lemma 1 (MS-FHE (SS)): Individual encryption primitives are semantically secure therefore making our MS-FHE also semantically secure.

Proof (1) In our assumption, public-key encryption primitive $\epsilon = \{KeyGen, Enc, Dec\}$ is semantically secure. Depending on ϵ , there is a construction of evaluate algorithm $Eval$ by the challenger to $\epsilon_i = \{KeyGen, Enc, Dec, Eval\}$ maintaining homomorphic computations of multiplication and addition. In situations where the evaluation key is public, the adversary

will be capable of computing Eval directly based on the public key pk to produce a ciphertext ψ with evaluation key ek . For that reason, MS-FHE is secure semantically. $\square$

In this setting, there is no collusion between participating entities, and DPs cannot communicate with each other until the decryption stage. The semantic security of MS-FHE should also enable the CSP to be probabilistic polynomially bounded in the processes of transferring individual ciphertext to the computational evaluator for computation. The cryptographic service provider should not necessarily have to possess computational power that is bounded since its only duty is to concatenate contributing ciphertext. Computational evaluator and data providers are unable to intercept any of the learning results. The confidentiality of the learning results is hereby assured. We, therefore, obtained the following lemma:

Lemma 2 In Algorithm 2, Algorithm 3, and Algorithm 4 privacy preservation for the following parameters, i.e., z^2, z^3, a^2, a^3 and W^1, W^2 (forward and backpropagation) is enforced leading to the avoidance of privacy leakages during the mathematical computations.

Privacy of MSDP model Computational evaluator is honest-but-curious capable of privately training the collaborative DNN MSDP model. On the other hand, MSDP has securely protected against systems malicious adversary as described in Section 4.2. Initially, if A_d is able to corrupt DA or CE to get access to offloaded datasets. A_d is unable to obtain the corresponding plaintext due to the presence of the IND-CPA of our MSDP scheme. Furthermore, A_d has corrupted some of the DP and has been able to obtain the sk_i, pk_i of these corrupted DP. As a result of the non-interactive and independent key generated by the DP, these diverse sk_i and

pk_i keys are uncorrelated. Therefore, the adversary A_d is incapable of decrypting the encrypted data.

7.2 Analyzing the ϵ -differential privacy

This subsection demonstrates the differential privacy of the aggregated database ($\mathcal{X}'$) with data records $r_i = \text{pub}(r) \parallel \text{sec}(r)$ in a disjointed dataset D' which is individually independent of the datasets $\{D_1, D_2, \dots, D_n\}$. The privacy level basically relies on the worst of assurances of individual analysis. A description of this circumstance is in the preceding theorem:

Theorem 2 (Parallel composition). *Let $\{D_1, D_2, \dots, D_n\}$ be n instrument, where individual instrument $\mathcal{M}_i (i \in [1, n])$ provides ϵ_i -DP. Let $\{D_1, D_2, \dots, D_n\}$ be an arbitrary mutually independent datasets with data records $r_i = \text{pub}(r) \parallel \text{sec}(r)$ of the input domain D . For a latest instrument $\mathcal{M}$, the sequence of $\mathcal{M}(\mathcal{M}_1(D_1), \mathcal{M}_2(D_2), \dots, \mathcal{M}_n(D_n))$ which provides $(\max_{1 \leq i \leq n} \epsilon_i)$ -DP.*

Proof (2) In our case, for any of the sequence r of outcomes $\mathcal{D}'_i \in \text{Rang}(\mathcal{M}_i)$, let $\mathcal{D}'_i$ be mechanism $\mathcal{M}_i$ applied to the dataset $\mathcal{D}_i$, i.e., $\mathcal{D}'_i = \mathcal{M}'_i(\mathcal{D}_i)$. The probability of the output $\mathcal{D}'_i$ from the sequence of $\mathcal{M}'_i$ is

$$\Pr[\mathcal{M}(A) = r] = \prod_i \Pr[\mathcal{M}'_i(\mathcal{D}'_i)] \quad (5)$$

Therefore, if ϵ is smaller than 1 then $e^\epsilon \approx 1 + \epsilon$. Based on Definition 2, we now have

$$\Pr[\mathcal{M}(A) = r] \leq \Pr[\mathcal{M}(B) = r] \times e^{\epsilon \times |A \boxplus B|}, \quad (6)$$

Due to the inequality in the triangle $\|A - B\| \geq \|r\|B - \|A - r\|$, and $\|A - B\| \leq |A \boxplus B|$, the $\boxplus$ denotes the symmetric difference between datasets A and B and $|A \boxplus B|$ also denotes the shifted count from A and B datasets, with the help of ϵ -DP, $\prod_i [\mathcal{M}'_i(\mathcal{A}_i)] = \mathcal{D}'_i] \leq \prod_i [\mathcal{M}'_i(\mathcal{B}_i)] = \mathcal{D}'_i] \times \prod_i e^{\epsilon \times |A_i \boxplus B_i|} \leq \prod_i [\mathcal{M}'_i(\mathcal{B}_i)] = \mathcal{D}'_i] \times \prod_i e^{\epsilon \times |A \boxplus B|}$. $\square$

7.3 Analysis of MSDP architecture

Concretely, our proposed MSDP is grounded on Multi-Scheme (MS) FHE ϵ which uses additional algorithm $uEvaluate$ such that given any model $\mathcal{C}$ and ciphertext, it returns a ciphertext c which can be decrypted. It is semantically secure in the standard model. Furthermore, we are able to demonstrate MSDP can overcome the attack from adversaries as explained in Section 3.5. Detailed analysis is given as follows:

- In the situation where A_d has corrupted the computational evaluator or data analyst to obtain the outsourced dataset, A_d is incapable of obtaining the resultant plaintext due to the presence of INC-CPA security of our MSDP architecture.
- On the other hand, when A_d is able to corrupt some of the DPs to pk or sk of these DPs, the independent keys generation coupled with non-interactivity of the data providers makes the multiple schemes or secret keys unrelated. Consequently, A_d cannot decrypt these encrypted data from the data providers.

Furthermore, MSDP is also capable of supporting ϵ -DP. The evaluation of some of the deep learning models on the aggregated database is a non-linear function, i.e., derivative operation, exponential operations, etc. Evaluation of these models directly in the encrypted setting is not possible; however, these non-linear models may be evaluated with fitting, an approximation of a polynomial, and interpolation since the value of the ciphertext setting is huge as compared to the evaluation on an unencrypted dataset. On this premise, MSDP has greatly improved the precision and productivity of the learning model. This is because MSDP architecture is capable of transforming all the public keys with the addition of noise to the aggregated database by the CE. The data analyst can, therefore, perform ϵ -DP on the aggregated database without privacy leakage.

8 Conclusion

We conceptually present a privacy-preserving deep neural network MSDP architecture for wearable Internet of Thing devices based on human activity recognition applications by the injection of statistical noise to the constructed aggregated database by the computational evaluator (cloud server), BN, and alternative technique for approximating nonlinear ReLU function. Compared to ultramodern and baseline frameworks, MSDP demonstrated a reduction of communication cost, reduction of computational cost, higher accuracy, and efficiency on the four most widely used public datasets. In our future paper, we will consider the privacy preservation of the massive amount of real-time human activity recognition datasets from these wearable devices while considering the adjustment of connection methods and kernel size.

Funding 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).

References

1. Zhang N, Yang P, Ren J, Chen D, Li Y, Shen X (2018) Synergy of big data and 5G wireless networks: opportunities, approaches, and challenges. *IEEE Wireless Communications*. <https://doi.org/10.1109/MWC.2018.1700193>
2. Zhang N, Yang P, Zhang S, Chen D, Zhuang W, Liang B, Shen XS (2017) Software defined networking enabled wireless network virtualization: Challenges and solutions. *IEEE Network*. <https://doi.org/10.1109/MNET.2017.1600248>
3. Chen D, Zhang N, Qin Z, Mao X, Qin Z, Shen X, Li XY (2017) S2M: A lightweight acoustic fingerprints-based wireless device authentication protocol. *IEEE Internet of Things Journal*. <https://doi.org/10.1109/JIOT.2016.2619679>
4. Qin Z, Hu L, Zhang N, Chen D, Zhang K, Qin Z, Choo KKR (2019) Learning-aided user identification using smartphone sensors for smart homes. *IEEE Internet of Things Journal*. <https://doi.org/10.1109/JIOT.2019.2900862>
5. Qin Z, Wang Y, Cheng H, Zhou Y, Sheng Z, Leung VCM (2018) Demographic information prediction: a portrait of smartphone application users. *IEEE Transactions on Emerging Topics in Computing*. <https://doi.org/10.1109/TETC.2016.2570603>
6. Freundlich RE, Freundlich KL, Drolet BC (2018) Pagers, Smartphones, and HIPAA: finding the best solution for electronic communication of protected health information. *Journal of Medical Systems*. <https://doi.org/10.1007/s10916-017-0870-9>
7. Wagh S, Gupta D, Nishanth C (2018) SecureNN: efficient and private neural network training. *IACR Cryptology EPrint Archive*
8. Mohassel P, Zhang Y (2017) SecureML: a system for scalable privacy-preserving machine learning. In: *Proceedings - IEEE symposium on security and privacy*. <https://doi.org/10.1109/SP.2017.12>
9. Yin C, Xi J, Sun R, Wang J (2018) Location privacy protection based on differential privacy strategy for big data in industrial internet of things. *IEEE Transactions on Industrial Informatics*. <https://doi.org/10.1109/TII.2017.2773646>
10. Xiong H, Qian M, Yanan Z (2020) Efficient and provably secure certificateless parallel key-insulated signature without pairing for IIoT environments. *IEEE Systems Journal*. <https://doi.org/10.1109/JSYST.2018.2890126>
11. Chen D, Zhang N, Lu R, Fang X, Zhang K, Qin Z, Shen X (2018) An LDPC code based physical layer message authentication scheme with perfect security. *IEEE Journal on Selected Areas in Communications*. <https://doi.org/10.1109/JSAC.2018.2825079>
12. Cheng X, Tang P, Su S, Chen R, Wu Z, Zhu B (2020) Multi-party high-dimensional data publishing under differential privacy. *IEEE Transactions on Knowledge and Data Engineering*. <https://doi.org/10.1109/TKDE.2019.2906610>
13. Cui L, Qu Y, Nosouhi MR, Yu S, Niu J, Xie G (2019) Improving data utility through game theory in personalized differential privacy. *Journal of Computer Science and Technology*. <https://doi.org/10.1007/s11390-019-1910-3>
14. Li P, Ye H, Li J (2017) Multi-party security computation with differential privacy over outsourced data. *Security, Privacy and Anonymity in Computation, Communication, and Storage China*. <https://doi.org/10.1007/978-3-319-72389-1-39>
15. Bogdanov D, Laur S, Willemson J (2008) Sharemind: a framework for fast privacy-preserving computations. <https://doi.org/10.1007/978-3-540-88313-5-13>
16. Bogdanov D, Niitsoo M, Toft T, Willemson J (2012) High-performance secure multi-party computation for data mining applications. *International Journal of Information Security*. <https://doi.org/10.1007/s10207-012-0177-2>
17. Pettai M, Laud P (2015) Combining differential privacy and secure multiparty computation. In: *ACM International conference proceeding series*. <https://doi.org/10.1145/2818000.2818027>
18. Goryczka S, Xiong L (2017) A comprehensive comparison of multiparty secure additions with differential privacy. *IEEE Transactions on Dependable and Secure Computing*. <https://doi.org/10.1109/TDSC.2015.2484326>
19. Roggen D, Calatroni A, Rossi M, Holleczeck T, Förster K, Tröster G, Lukowicz P, Bannach D, Pirkel G, Ferscha A, Doppler J, Holzmann C, Kurz M, Holl G, Chavarriaga R, Saghah H, Bayati H, Creatura M, Millán JR (2010) Collecting complex activity datasets in highly rich networked sensor environments. *INSS 2010 - 7th International Conference on Networked Sensing Systems*. <https://doi.org/10.1109/INSS.2010.5573462>
20. Reiss A, Stricker D (2012) Introducing a new benchmarked dataset for activity monitoring. *proceedings - international symposium on wearable computers, ISWC*. <https://doi.org/10.1109/ISWC.2012.13>
21. Anguita D, Ghio A, Oneto L, Parra X, Reyes-Ortiz JL (2013) A public domain dataset for human activity recognition using smartphones. In: *ESANN 2013 proceedings, 21st european symposium on artificial neural networks, computational intelligence and machine learning*
22. El-Yahyaoui A, Kettani MDECE (2019) An efficient fully homomorphic encryption scheme. *Int. J. Netw. Secur.* 21(1):91–99. [Online]. Available: <http://ijns.femto.com.tw/contents/ijns-v21-n1/ijns-2019-v21-n1-p91-99.pdf>
23. Hoffstein J., Pipher J, Silverman JH (1998) NTRU: a ring-based public key cryptosystem. In: *Algorithmic number theory, third international symposium, ANTS-III, Portland, Oregon, USA, June 21-25, 1998, Proceedings pp 267–288*. <https://doi.org/10.1007/BFb0054868>
24. López-Alt A, Tromer E, Vaikuntanathan V (2012) On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption. In: *Proceedings of the 44th symposium on theory of computing conference, STOC 2012, New York, NY, USA, May 19 - 22, 2012, pp 1219–1234*. <https://doi.org/10.1145/2213977.2214086>
25. Dwork C (2010) Differential privacy in new settings. In: *Proc. 21st annu. ACM-SIAM symp. discret. algorithms*. pp 174–183. <https://doi.org/10.2307/2374806>
26. Mukherjee P, Wichs D (2016) Two round multiparty computation via multi-key FHE. In: *Advances in cryptology - EUROCRYPT 2016 - 35th annual international conference on the theory and applications of cryptographic techniques, Vienna, Austria, May 8-12. Proceedings, Part II, 2016, 9666, pp 735–763*. <https://doi.org/10.1007/978-3-662-49896-5-26>
27. Mukherjee P, Wichs D (2015) Two round MPC from LWE via multi-key FHE. *IACR Cryptol. ePrint Arch.*, 2015, 345. [Online]. Available: <http://eprint.iacr.org/2015/345>
28. Abuhasel KA, Khan MA (2020) A secure industrial internet of things (IIoT) framework for resource management in smart manufacturing. *IEEE Access* 8:117354–117364. <https://doi.org/10.1109/ACCESS.2020.3004711>
29. Wei K, Zhang L, Yi G, Jiang X (2020) Health monitoring based on internet of medical things: architecture, enabling technologies, and applications. *IEEE Access* 8:27468–27478. <https://doi.org/10.1109/ACCESS.2020.2971654>
30. Gentry C (2009) Fully homomorphic encryption using ideal lattices. In: *Proceedings of the forty-first annual ACM symposium on theory of computing*

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.