S-PPOC: Multi-scheme Privacy-Preserving Outsourced Classification

Kwabena Owusu-Agyemeng, Zhen Qin,Hu Xiong,Tianming Zhuang, Liu Yao, and Zhiguang Qin
(Corresponding author: Kwabena Owusu-Agyemeng)

School of Information and Software Engineering, University of Electronic Science and Technology of China
No. 2006, Xiyuan Ave, West Hi-Tech Zone, Chengdu, Sichuan 611731, China
Email: cooljacko@gmail.address

(Received Mar. 4, 2020; Revised and Accepted Oct. 12, 2020; First Online Apr. 20, 2021)

Abstract

Human activity recognition HAR has gained tremendous research attention aiming at understanding the human activities in the field of ubiquitous healthcare. Deep learning has progressively been applied to extract, constructed features, and train models accurately for high-level data representations required for medical diagnosis. However, these deep learning models are affected by efficiency, accuracy and are also confronted with data privacy dilemmas. This paper proposes an architecture dubbed S-PPOC, a combination of batch normalization and polynomial approximation of Rectified Linear Unit (ReLU) activation function for privacy-preserving classification. This is to enforce both the confidentiality of the manipulated datasets and the model's efficiency to address these problems successfully. With the application of S-PPOC, the computational evaluator is capable of securely training a classification model over data encrypted with different fully homomorphic encryption schemes contributed by multiple Data Providers. Our scheme is proven to be secured in the honest-but-curious threat model compared to other existing cutting-edge privacy-preserving deep learning models.

Keywords: Batch Normalization; Classification; Human Activity Recognition; Privacy-Preserving; ReLU Activation Function

1 Introduction

Human activity recognition [12, 24] based on Wireless Body Area Network [40,41] (WBAN) has gained tremendous research attention in the field of ubiquitous healthcare [17, 32]. WBAN [33] as an extension of our traditional wireless sensor networks (WSN) through Human activity recognition detects, interprets and monitors human behavior, activity types and patterns, either occasional or habitual with the aid of wearable devices attached to the human body with the aim of transforming lives [20, 23, 28]. Numerous real-world applications such as medical diagnosis [13,24], athletic competition, nursing and smart homes has exploited and successfully benefited from the potential of the huge amount of data generated from these sensor-based human activity recognition.

To provide useful information to data owners and patients, storage and processing requirements of the massive amount of data generated by sensor-based HAR systems still remain an imperative task in the ubiquitous healthcare space. In the scenario of personal healthcare, fitness records monitored by WBAN [34], specific deep leaning models are trained on aggregated datasets from different parties for better representations and accurate diagnosis, which may be expensive or complicated for a single data owner to achieve. Fortunately, cloud computing comes in handy as a novel computing paradigm to eliminate the need to maintain expensive computing resources, dedicate storage and software at a nominal management cost. Recently, patients and hospitals have exploited the promising potential of cloud computing [10, 39, 45] to remotely store and train their deep learning models.

Arguable, deep learning models has been applied on the massive data generated by WSNs [49] through their low-capacity sensor to efficiently solve the evolving challenges during big data processing and complex representations in Human Activity Recognition. However, there are still prevalent deficiencies confronting HAR models:

1) Better representations of the models requires data aggregated from different parties which may be expensive or completed for a single party to achieve.
2) Security [4] of the aggregated datasets.
3) Privacy and security of the model. In addition, sensor nodes of WBAN [48] have challenges with energy consumption of these wearable devices which is outside the scope of this paper.

Furthermore, training of deep learning models requires access to the unprotected datasets which is customarily privacy sensitive. Unfortunately, cloud-based classification would not be preferred by the data owners without guarantee for confidentiality, privacy and security [6, 7, 16, 51]

of the outsourced datasets. Since the threats in the cloud jeopardize some of the basic security requirement. Therefore, it is essential to protect these confidential data before outsourcing any computation to the untrusted third party [29, 46]. One of the promising solutions is for users to encrypt their private data before outsourcing computations to the Data Service Provider (DSP). However, due to organizational policies mutually untrusted parties would like to encrypt their data with different fully homomorphic encryption schemes before the untrusted third party can aggregate encrypted datasets and perform any computations. The Multi-key FHE [30] offers a suitable scheme for aggregating the datasets under different keys in such domains. This powerful scheme has been integrated with deep learning in the pioneering architecture of [25], known as Multi-key privacy-preserving deep learning MK-PPDL which built a convolutional neural network on Multikey fully homomorphic encryption to process inference queries.

Existing endeavors on collaborative privacy preservation in outsourcing computations are mostly based on encrypting the datasets with same public keys [21, 22]. Considering a more practical scenario where outsourced datasets are from diverse locations and parties. For example, the network infrastructure of a communication network may belong to multiple providers; Base stations of a sensor network may be owned by multiple medical institutions. To be more precise, we are considering the following scenario in this work.

- For n mutually non-colluding data providers $P_1, P_2, \cdots, P_n$, every data owner $P_i (i \in [1, n])$ encrypt private data with their respective scheme before outsourcing the ciphertext to a Data Service Provider before allowing the Computational Evaluator to concatenate the datasets before any computations are performed.
- Computational Evaluator performs part of the computational classification over the concatenated data. All contributed data and intermediate results still remains confidential.
- There is no interaction between Data Owners, Data Services Provider and Data Providers.
- Immediately the classifier is trained, the computational evaluator can respond to the client query without learning any of the intermediate results.

In this domain, we focuses on multi-scheme privacy-preserving outsourced deep learning classification over data encrypted with *different encryption schemes or even different public keys*.

The multi-scheme privacy-preserving outsourced classification models are confronted with three fundamental issues:

P1. The MK-FHE scheme in [25] was built upon provable secure NTRU encryption and had a limitation that the maximal number of participants in a computation had to be known at the time a key was generate. Thus making it computationally expensive and undesirable for large-scale *deeper* neural networks.

P2. Classification over sensitive data is extremely complicated, since it involves additions, multiplications and the nonlinear (ReLU, Sigmoid) polynomial approximations, which leads to low efficiency and degraded accuracy in practice.

P3. Over the past decade, numerous privacy-preserving collaborative deep learning frameworks with the polynomial approximation of activation functions have been developed [43]. Training is unstable due to approximated polynomial activation functions but only support inference. Privacy-preserved training is considered in [11] which also utilizes polynomial approximation (e.g. Standard Chebyshev) to outwit the difficulty of activations. Thus, it suffers from accuracy loss and training instability.

In this paper, we propose a novel architecture dubbed **M**ulti-**S**cheme **P**rivacy-**P**reserving **O**utsourced deep learning **C**lassification in Cloud Computing(**S-PPOC**). This is to resolve the three outlined concerns in the existing framework [25]. The inherent strategy is to demonstrate that, Computational Evaluator is capable of utilizing the outsourced ciphertext for the evaluation of privacy-preserving classification model for deep neural network with depth greater than two and respond to Data Requesters predicted query. To end up with a construction being FHE friendly while keeping accuracy at a higher level, the multiplicative depth of the deep neural network is to be maintained reasonable low.Hence, our technique is much more efficient than the general secure multi-party evaluation [9, 25] which is impractical when subjected to larger number of trails. In addition, we present a security analysis of our proposed S-PPOC.

We advance the state-of-the-art technique of improving [9, 25] with the following main contributions:

- We propose a secure S-PPOC, which allows the data analysts to make privacy queries with higher accuracy predictions for patient's diagnosis without leaking sensitive information. In S-PPOC, the massive amount of HAR datasets from different data providers are securely stored and aggregated in the cloud server and can be used to build classifiers with the aid of the deep neural network. In this setting, the cloud server is not required to choose a type of fully homomorphic encryption scheme for data providers, rather DP can encrypt their data with their preferred choice of FHE encryption scheme. With the aid of the classifiers on the cloud server, data analyst can perform privacy-preserving disease diagnosis.
- To improve efficiency and circumvent the classification errors that dramatically degrade the accuracy

of the models, S-PPOC combine the polynomial approximation of ReLU [14] activation function with batch normalization without information leakage to facilitate secure outsourced multi-party computation of ciphertexts.

- To validate the efficiency and accuracy of S-PPOC, we demonstrate the theoretical analysis and experimental simulations that indicate the feasibility and practically secure model required to achieve the privacy-preserving classification in the semi-but-honest threat model.

The rest of the paper is organized as follows. In Section 2, we provide an overview of the related work. Section 3 gives some notations and presents the definition of homomorphic encryption and classification related to this paper. The system architecture is given in Section. 4. The collaborative privacy-preserving classification system based on the Multi-scheme fully homomorphic encryption scheme is illustrated in Section 5, while analyzing security in Section 6. Finally, the whole paper is concluded in Section 7.

2 Related Works

Most of the existing privacy-preserving methods in machine learning are based on secure multiparty (SMC) computations, fully homomorphic encryption, garbled circuits or combination of both. Concretely, the structure of privacy-preserving machine learning can basically be divided into two main categories:

1) Training phase, which requires an efficient algorithm to solve the optimization problem by using secure samples;

2) The classification phase, which predicts the classification of new samples. The efficiency of this proposals strongly depends on the complexity of the deep neural network *i.e.* the approximation of the activation function, number of layers, and number of neurons per each of the layers for the classification function.

Previous endeavors focused on the first or the second categories. Our proposed framework is directed towards the protection of the privacy of the training datasets, parameter of the classifiers and the intermediate results.

2.1 Privacy-Preserving Training

Several related works on the problem of privacy-preserving deep neural network learning [18] have recently been presented. For example, Graepel *et al.* established that some of the basic machine learning algorithms, such as classification can be computed efficiently over a small scale encrypted datasets. However, as the input size grows the efficiency will also be degraded rapidly. Theoretically, most of the issues confronting multiparty privacy preserving deep learning can be resolved with the aid of secure multi-party computation (SMC) protocols, but the extremely computational complexities and high communication usually makes it impractical, whiles the two-party case is not an exception. In [47], with the adoption of double homomorphic encryption scheme(BGN), Yuan *et al.* proposed a system in which the training phase was securely delegated to the data service provider for efficient computations in the multi-party scenario. In multiparty scenario, back-propagation network learning has been one of the widely used learning methods. In [3, 50] applied BGN in other to support secure computation operations and also realized a high-order back-propagation algorithm computation model training in data service provider. Chen *et al.* [2] also propose a privacy preserving back-propagation network learning algorithm for two-party scenarios with the use of secure scalar and secrete sharing to protect data and the intermediate results against leakages during the training of the deep neural network model. Though this scheme is applied in the two-party settings, however extending it to the multi-party models might not be trivial. In [43], Takabi *et al.* proposed a privacy-preserving back-propagation algorithm for the multi-party deep learning over arbitrarily partitioned datasets base on BGN homomorphic encryption. One of the bottlenecks of this scheme is where all the data owners must stay online and work interactively do control and noise in the ciphertext and also to decrypt the ciphertext of the intervening parameters in each iteration.

2.2 Privacy-Preserving Classification

Classification is one of the most fundamental task in deep learning and data mining, let consider prediction of medical diagnosis with generated data from wireless sernsor networks [5, 19] (WSN), models generated from existing data and if new patient record are similar to the existing data used for the model, then we can obtain a correct prediction for the new patients diagnosis. However, information from a predictors datasets are sensitive, these include, temperature, gender, age, medical history and symptoms. However, to preserve the privacy of the patients datasets, it is important to propose a privacy-preserving medical diagnosis model. Deep neural network model generalization performance is highly stimulated by the quality and volume of datasets used in the training process. As a result of this, privacy-preserving machine learning via secure multiparty computations (SMC) provides a promising solution by allowing multiple entities to train various models, researchers have recently proposed SecureML, CryptoDL, CryptoML, and schemes for secure delegation of iterative collaborative machine learning to the third party cloud servers. In MK-PP, which is the most popular scheme in the collaborative privacy-preservation deep learning settings is based on multi-key fully homomorphic encryption. In this scheme data owners encrypts their own datasets with different public keys and uploads them to the data service provider whiles the cloud server implement the

deep learning algorithm by the use of multi-key FHE. Based on the related works described above, it is obvious that most of the deep learning secure multiparty based approaches refer to semi-homomorphic encryption or multi-key fully homomorphic encryption.

The existing major interesting challenges confronting these scheme is whether all the FHE schemes from the data providers can be made multi-key to enable deep learning privacy preservation computations and is it also possible to homomorphically evaluate a classifier $\mathcal{C}$ on a ciphertext. the adaptation of a classification algorithm to render it compatible with the fully homomorphic encryption scheme whiles maintaining accuracy and efficiency. Lastly, most of the existing deep neural networks and its utility is very low with non-linear layers more than 2 (since it is predominant in current applications).

3 Preliminaries

This section defines some notations and review some cryptographic scheme used in our architecture. The notations are listed in Table 1 Fully homomorphic encryption (FHE) supports meaningful unlimited addition and multiplication computations over encrypted data with results of addition and multiplications which is equivalent to computations over plaintext by the application of the corresponding ciphertext directly without decryption.

Table 1: Notations of our protocol

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

3.1 Homomorphic Encryption

FHE scheme is $\varepsilon_i = (KeyGen_i, Enc_i, Dec_i, Eval_i)$ with a Key generation algorithm $KeyGen$ takes a parameter λ as input and outputs a public key pk_i and a private key pk_i *i.e.* $(pk_i,\ sk_i) \leftarrow KeyGen(\lambda)$. The encryption algorithm Enc_i takes as input public key pk_i and plaintext x and returns the corresponding ciphertext ψ *i.e.*, $\psi \leftarrow Enc(pk_i, x)$. Decryption algorithm Dec_i takes the private key sk_i as input and ciphertext ψ and returns x as plaintext, *i.e.* $\psi \leftarrow Dec(pk_i, \psi)$. Evaluation algorithm $Eval$ takes pk_i as input, a circuit $\mathcal{C} \in \mathcal{C}_{\prod}$, and a tuple of ciphertext $\{\psi_1, \psi_2, \cdots, \psi_n\}$ and returns a ciphertext ψ_i *i.e.* $c \leftarrow Eval(pk, \mathcal{C}, \psi_1, \psi_2, \cdots, \psi_n)$,such that $\mathcal{C}(x_1, x_2, \cdots, x_n) = Dec(sk, \psi)$, where $\mathcal{C}_{\prod}$ is a permitted circuit set and $\psi_i \leftarrow Enc(pk, x_i)$, $i \in [1, n]$. The circuits $\mathcal{C}(\in \mathcal{C})$ might be any circuit with different functions.For example $\mathcal{C}$ is decryption circuit $D_{\prod}(D_{\prod} \in C_{\prod})$. The decryption operation can be performed by the Eval.$\prod$ is therefore bootstrappable in this instance.

3.2 Classification in Machine Learning

Most of the existing machine learning algorithms are basically used for classification [15]. Classification models can be categorized into two major phases: inference stage and decision stage. During the inference stage, training sets are used to learn a model for the computation of the feature vectors whiles in the decision stage these feature vectors are applied for optimal class assignments. On the other hand, classification models can also be viewed as implementing a set of discriminant functions, $f_1(x), \cdots, f_n(x)$ mapping each input x directly inot one of the N class labels, denoted by B_n, where the input vector x with k attributes: $x = (x_1, x_2, \cdots, x_k) \in \mathbb{R}^k$. we therefore choose B_n if $f_n(x) = max f_i(x)$, not B_n.

Training in the classification algorithm involves two main groups: supervised and unsupervised. Supervised classifiers contains targeted features or labels, whiles the unsupervised classifiers experience a dataset containing many feature samples helping the algorithm to learning useful knowledge of the structure of these datasets.

4 Problem Scenario

Consider a scenario in a Ubiquitous healthcare system: A healthcare center has created a deep learning solution which is capable of assisting medical diagnosis, financial discovery and financial review of a patient. Interested hospitals might want to improve the model and also take advantage of the services offered by the model. This can be achieved by contributing their data for the collaborative training of the model. Privacy issues and fear of reverse-engineering of their solutions increases the unwillingness of the client to send their data to the other parties, therefore making this server-sided services impossible.

To preserve the privacy of Data Providers data, all parties would have to crowd-source their data in an encrypted form in such a way that only the Data Provider could decrypt. In this settings the client due to organizational policies is required to encrypt their data with their choice of encryption scheme or even keys different from the other Data Providers. Under a typical encryption scheme, the organization could not process this input in any meaningful way.In this domain, basic solution to this problem would require the Data Provider's input is not revealed to the Data Service Provider and the weights of the model are also not revealed to the client. Data Service Provider should be able to support arbitrary deep models with common operations which include CNN and ReLU.Our approach is efficient and capable of preserving the privacy of Data Provider's data without sacrificing security or accuracy with the aid of fully homomorphic encryption (FHE).

4.1 System Model for S-PPOC

In this section, we give some intuition behind our multi-scheme privacy-preserving classification in the cloud S-PPOC. A secured multi-party deep learning model follows the insight of prior works [25]. In order to offer, confidentiality, privacy and security of the data, parameters and models of the neural network whiles improving generalization of the model, we adopt *Multi-scheme fully homomorphic encryption,DBLP:journals/iacr/LiL13* (MS-FHE). We incorporate the idea of outsourcing technique with each of the Data Providers encrypting their datasets with their choice of fully homomorphic encryption. Our protocol consist of the following components and entities.

- *Data Providers*(DP): Each of the Data providers $P_i \in [1, n]$ outsourced their data to the Computational Evaluator CE for storage and also allow computational operations on these stored datasets. The datasets may contain sensitive information. The Data Providers $P_i \in [1, n]$ encrypts their sensitive data before outsourcing it to the CE to prevent privacy leakages.

- *Honest-but-curious Computational Evaluator*(CE): Computational Evaluator provides services such as storage and response to queries for Data Providers and Data Requestors. CE can basically represent a medical institution in this scenario. The CE stores the datasets encrypted with different fully homomorphic encryption or even different public keys chosen independently by the Data Providers. The CE therefore aggregates the ciphertext and uses the concatenated ciphertext to construct a classification model. The trained classifier is then used by the CE for data analytics or predications for the Data Requestors query.

- *Honest-but-curious crypto service provider* (CSP): The Crytpto Service Provider is capable of providing only crypto services to the Data Requestors. For example, the CSP is responsible for handling the ciphertext and also performs the decryption of the ciphertext sent by the CE.

- *Data Requestors* (DR): The DR is capable of gathering feature vectors of their records. In situations where DR wants to query the CE for prediction service securely, then DP encrypt their queries before outsourcing to the CE.

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

4.2 Threat Model

In this settings the entities involved in the privacy-preserving process *i.e.* Data Providers, Data Requestors, Computational Evaluator and Crypto Service Provider are expected not to collude with each other. S-PPOC is based on honest-but-curious model, in this settings malicious attackers may exist around Data Providers and steal information during outsourcing of training datasets. Then, we consider the Computational Evaluator to be curious-but-honest. During the training process, Computational Evaluator may be curious about participant's local datasets. CP may be strictly following the training protocol whiles trying to violate and disclose participant's sensitive information.

4.3 Design Goals

As a privacy-preserving collaborative deep learning model, S-PPOC allows the Computational Evaluator to process and construct a privacy-preserving classifier over the collaborative Data Providers and response to the Data Requestors prediction queries. S-PPOC should meet the following requirement to address the security and adversary models:

- *Classifier accuracy*: S-PPOC should be capable of classifying correctly for every query from the Data Requestors whiles making accurate predictions with high probabilities.

- *Privacy-Preservation*: Provision of privacy guarantee by the system should be assured without disclosing confidential information about Data Provider's and the classification model. To achieve this security goal, training and prediction stage should be performed in the encrypted settings. The Data Requestor is the only who will be capable of obtaining the decrypted intermediate results by the application of the private key after the Computational evaluator has responded to predictive query. The Crypto Service Provider is not known and thereby hidden from the Data Providers.

- *Flexibility*: In S-PPOC, crypto service provider is not a fixed service provider. In this domain, the CSP can be different parties or institutions publishing their corresponding different schemes or different public keys based on different functions or motivations.

5 S-PPOC Scheme

5.1 Main Idea

S-PPOC scheme focuses on the training of a classification model over aggregated datasets from multiple Data Providers with the aim of offering a confidential prediction services for Data Requestors with this classification model. In this instance, a set of n mutually non-colluding DPs $P_1, P_2, \cdots, P_n$ outsourced their encrypted data to the CE for storage whiles allowing it to perform some computational operations on these concatenated datasets. In other to support the computation over the encrypted

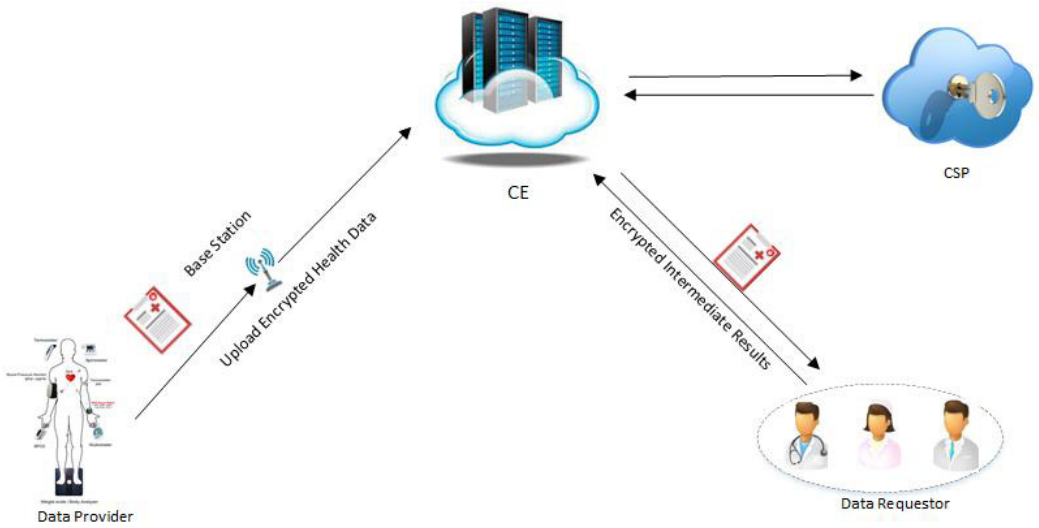

Figure 1: System model

data with possibly different fully homomorphic encryption schemes or with even different public keys, Multi-scheme Fully homomorphic encryption scheme will be used as our privacy-preserving technique to concatenate the encrypted dataset from DP before outsourcing to the Computational evaluator. Application of these outsourced concatenated ciphertext enables the CE to construct a classification model whiles storing and maintaining the model in an encrypted form. The classification model in the CE is therefore ready to respond to queries from DP.

5.2 Overview of S-PPOC Scheme

This section gives an overview of the S-PPOC scheme and demonstrate how to achieve the data outsourcing and secure classification.

- *Secure Data Outsourcing*: Encrypted data is been outsourced to the CE. DP are required to encrypt their data to preserve the confidentiality of the sensitive datasets based on their choice of Fully Homomorphic encryption. In this paper, the method for the aggregated confidential data processing is based on [27] ε^i which is capable of concatenating all the different public keys into ciphertext under same public key.

- *Secure training*: CE then used the outsourced concatenated datasets to build a classification model. The ciphertext encrypted with possibly different keys requires the CE and CSP to jointly train the classification model. The model is stored in an encrypted form in the CE after classification. CE then uses this model to provide secure prediction services to the DP query.

- *Secure Prediction*: Computational Evaluator CE run a classifier, denoted as $\mathcal{C}$ over encrypted database $\text{Enc}(\mathcal{X})$ and returns the result $\psi \leftarrow Evaluate(\mathcal{C}, \{\langle pk_i \psi_i \rangle\})$ which is finally send to the Data Requestor.

- *Secure Extraction*: One the Data Requestor obtains a prediction $\psi \leftarrow Evaluate(\mathcal{C}, \{\langle pk_i \psi_i \rangle\})$, the data is then decrypted with their private key sk_i to get the prediction.

5.3 Detail Design of S-PPOC

This section present a more detailed description of S-PPOC scheme which is basically divided into three phases: Privacy-preserving training classified, Generating Privacy-preserving prediction query from Data Requestors, preserving-preserving extracting results. The overall construction of our scheme is shown in Algorithm 3.

Stage 1: Privacy-preserving training of the classifier. In this section, we discuss the proposed S-PPOC model. The main work is directed towards the training of classifier over encrypted setting with data contributed from multiple Data Providers $\{P_1, P_2, \cdots, P_n\}$. For example, Alice encrypting Db_1 [3], Bob encrypted Db_2 with [42] whiles Eve also encrypt Db_3 with [8]. In this scenario, all parties are encrypting their data with different fully homomorphic encryption scheme. For a lucid discussion, initially a setup process for all the schemes is independently initialized and distribute the system security parameters. Meanwhile, in this stage, according to different target or motivation, determine a Crypto Service Provider entity with special function. Therefore, once the CSP is confirmed. It then distribute a public or private key pairs $\{pk_i, sk_i\}$.

In this process, each of the Data Providers independently generates a pair of public and pri-

vate keys $pk_i, sk_i \leftarrow KeyGen(1^{\lambda})$. Then they encrypts their secrete fields to generate cipher: $r_i = pub(r_i)||Enc(pk_i sec(r_i)$. All Data Providers outsource their encrypted data ψi, along with respect to encryption key pk_i to Computational Evaluator. CE construct an encrypted database $Enc(\mathcal{X}) \triangleq \{\langle pk_i, \psi_i \rangle\}$ from each Data Provider.

Polynomial approximation of ReLU. Our proposed model S-PPOC for a privacy-preserving classification on deep neural network has three major requirements: data privacy, efficiency with reasonably low multiplicative depth and accuracy which is close to the state-of-the-art convolutional neural network. The ReLU function and max pooling functions which have a high multiplicative depth in the CNN architecture are incompatible with the efficiency requirement of S-PPOC.

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	$0.1249 + 0.5000X + 0.3729X^2 - 0.0410X^4 + 0.0016X^6$

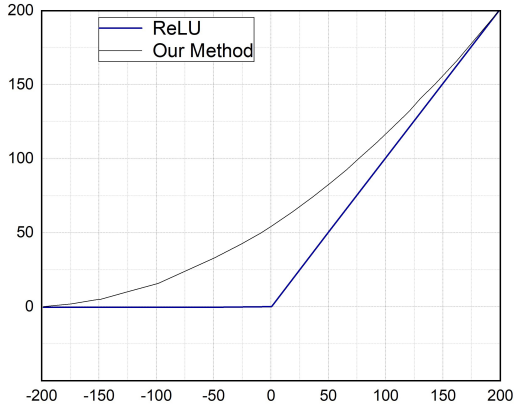

Figure 2: Approximaiton of ReLU in the 2 degree

In this stage, we modify the CNN model by replacing the high multiplicative depth layers *i.e.* ReLU and Max pooling by a low multiplicative depth polynomial layers into the CNN model, with reduction in degradation of the accuracy of the classification. Our aim is to approximate the ReLU function. We therefore focus on approximating the derivative of the ReLU function instead of approximating the ReLU function. The derivative of the activation function is like step function and is non-differentiable in point 0. In situations where the function is continuous or non-infinitely differentiable function we can approximate it more accurately. We therefore simulate the structure of the derivative of the ReLU function. Sigmoid activation function is bounded, continuous and infinitely differentiable function, it′s structure is like the derivative of the ReLU function in the large intervals. We therefore approximate the sigmoid function with the polynomial, find the integral of the polynomial and use it as the activation function. To achieve our goal, we combine the polynomial approximation of the ReLU with batch normalization [14] whiles replacing the max-pooling by the sum-pooling which has a null multiplicative depth. On the other hand, before each ReLU layer, we add a batch normalization layer in order to have a restricted stable distribution at the entry of the ReLU. The batch normalization layers are therefore added to the training and the classification stage to avoid high accuracy degradation between the training stage and the classification stage due to numerous modifications to the CNN model.

Algorithm 1: Batch Normalizing Transformation

Input: Values of x over a mini-batch: $\mathcal{B} = \{x_1, \cdots, m\}$;Parameters to be learned:γ, β

Output: $\{y_i = BN\gamma, \beta(x_i)\}$

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

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

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

$y_i \leftarrow \gamma\hat{x}_i + \beta \equiv BN_{\gamma,\beta}(x_i)$ // scale and shift

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

Stage 2: Generating Privacy-preserving prediction query. On receiving the query $\mathcal{C}$ from the Data Provider, the Computational evaluator generates a response by evaluating the query on the encrypted ciphertext. Using Evaluate algorithm, where the circuit $\mathcal{C}$ being evaluated is the query. This yields an encryption of the results of the deep learning process:$\psi_i \leftarrow Evaluate(\mathcal{C}, Enc(\mathcal{X}))$ $= Evaluate(\mathcal{C}, \{\langle pk_i, \psi_i \rangle\}_{i=1,\cdots,n}.|$.

Stage 3: Privacy-preserving extracting result. Once the transformed query results have been computed, the Computational Evaluator sends it back to the DP. When the Data Provider receives the encrypted query. The ciphertext ψ_i decrypts to $\mathcal{C}(\mathcal{X})$. with $Decrypt(sk_1, \cdots, sk_n; \psi) = \mathcal{C}(X)$.

Algorithm 2: Privacy-Preserved Forward Propagation

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

for $i = 1, 2, \cdots, i_{max}$ **do**
  for $i = 1, 2, \cdots, (n-1)$ **do**
    Compute;
    $z^{(2)}_{j_1 j_2 \cdots j_n} = W^{(1)}_{\alpha} \cdot X + b^{(1)}_{j_1 j_2 \cdots j_n}$;
    $a^{(2)}_{j_1 j_2 \cdots j_n} = f(z^{(2)}_{j_1 j_2 \cdots j_n})$;
    $z^{(3)}_{i_1 i_2 \cdots i_n} = W^{(2)}_{\beta} \cdot a^{(2)} + b^{(2)}_{i_1 i_2 \cdots i_n}$;
    $h_{(i_1 i_2 \cdots i_n) W,b}(X) = a^{(3)}_{i_1 i_2 \cdots i_n} = f(z^{(3)}_{i_1 i_2 \cdots i_n})$;
  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: $\phi = \{W^1, W^2, b^1, b^2\}$

for $i = 1, 2, \cdots, i_{max}$ **do**
  for *example* $= 1, 2, \cdots, N$ **do**
    for $i_n = 1, 2, \cdots, I_1 \times \cdots, I_N$ **do**
      Calculate;
      $\sigma^{(3)}_i = (a^{(3)}_i \cdot (1 - a^{(3)}_i)) \cdot \sum_{j=1}^{I_1 \times I_2 \times \cdots \times I_N} g_{ij}(a^{(3)}_j - y_j)\ \sigma^{(2)}_{j_1 j_2 \cdots j_n} = (\sum_{i_1=1}^{I_1} \cdots \sum_{i_n}^{I_n} w^{(2)}_{\lambda j_1 j_2 \cdots j_n} \cdot \sigma^{(3)}_{i_1 i_2 \cdots i_n}) f'(z^{(2)}_{j_1 j_2 \cdots j_n})$;
      $i_n = 1, 2, \cdots, I_N$
      $\Delta b^{(2)}_{i_1 i_2 \cdots i_n} = \Delta b^{(2)}_{i_1 i_2 \cdots i_n} + \sigma^{(3)}_{i_1 i_2 \cdots i_n}$
      $\Delta w^{(2)}_{i_1 i_2 \cdots i_n j_1 j_2 \cdots j_n} = \Delta w^{(2)}_{i_1 i_2 \cdots i_n j_1 j_2 \cdots j_n} + a^{(2)}_{j_1 j_2 \cdots j_n} \cdot \sigma^{(3)}_{i_1 i_2 \cdots i_n}$
      $b^{(1)}_{j_1 j_2 \cdots j_n} = \Delta b^{(1)}_{j_1 j_2 \cdots j_n} + \sigma^{(2)}_{j_1 j_2 \cdots j_n}$
      $\Delta w^{(1)}_{j_1 j_2 \cdots j_n i_1 i_2 \cdots i_n} = \Delta w^{(1)}_{j_1 j_2 \cdots j_n i_1 i_2 \cdots i_n} + x_{i_1 i_2 \cdots i_n} \cdot \sigma^{(2)}_{j_1 j_2 \cdots j_n}$
  $W = W - \eta \cdot (\frac{1}{N} \Delta w)$;
  $b = b - \eta \cdot (\frac{1}{N} \Delta b)$;

6 Security Complexity Analysis

The privacy characteristics of S-PPOC is analyzed against possible attacks by various entities involve in our privacy-preserving model. We define the semantic security as follows:

Definition 1. *(Semantic Security(SS), IND-CPA). A public-key encryption scheme ε = (KeyGen, Enc, Dec) is semantically secure, if for any stateful PPT adversary $A = (A_1, A_2)$, its advantage $Adv^{SS}_{\varepsilon.A}(K) := |Pr[Exp^{SS}_{\varepsilon.A}(K) = 1] - \frac{1}{2}]$ is negligible, where the experiment $Exp^{SS}_{\varepsilon.A}(K)$ is defined as follows:*

$Exp^{SS}_{\varepsilon.A}(K)$

$b \leftarrow 0, 1$

$(pk, sk) \leftarrow keyGen(1^k)$

$(m_0, m_1) \leftarrow A_1(pk)$

$c \leftarrow Enc_{pk}(m_b)$

$b' \leftarrow A_2(c)$

if $b' = b$. return 1:

else, return 0

The messages m_0, m_1 are called chosen plaintext, whiles c is called the challenge ciphertext. The length of two messages are required which must be equal, *i.e.* $|m_0| = |m_1|$. If the messages length is not equal. If the message length is not equal, A_2 can pad the shorter message into the equal length of the other. Thus, from the Definition 1, a property of semantic security can be obtained as follows

Property 6.1: Given the ciphertext, any computation be efficiently performed on the plaintext, can also be efficiently performed with the ciphertext.

Honest-but-curious crypto service provider. For the honest-but-curious crypto service provider CSP, it uses the private key sk_i to get blinded plaintext. Since the CE randomly chooses some randomness as blinded factor, and adds it to a fully homomorphic ciphertext before outsourcing to the CSP. Hence, CSP cannot gain any additional information on the blinded ciphertext.

Honest-but-curious computational evaluator. We therefore give a security analysis for our proposed model S-PPOC, proving that it is semantically secure.We assume that an adversary A chooses two plaintexts $m_0 = (m_{01}, m_{02}, \cdots, m_{0k})$, $m_1 = (m_{11}, m_{12}, \cdots, m_{1k}) \in P = [0, 1]$, and some circuit $\mathcal{C} \in \mathcal{C}$ with size $k = play(k)$.

Then A sends two plaintext m_0, m_1 and circuit $\mathcal{C}$ to the honest-but-curious computational evaluator CE (the challenger). The DSP tosses a fair coin $b \in [0.1]$, and outputs $\psi^* \leftarrow Evaluate(\mathcal{C}, pk_i, \psi_i, y_{b1}, y_{b2}, \cdots, y_{bk})$ where $x_{bi} \leftarrow Encrypt(pk, m_{bi})$. However, A knew the encrption x_{bi} and circuit $\mathcal{C}$, it then compute the Evaluate. This shows that the role of A and CE are the same. The CE only guesses the encrypted plaintext correctly with negligible advantage, even though some of the encrypted datasets are stored with the same plaintext. Based on the Property 6.1 we obtain the following theorem.

Theorem 1. *The S-PPOC scheme represented in Section 5 is semantically secure, if only the uderlying public encryption scheme is semantically secured.*

Algorithm 4: Overall Scheme of S-PPOC

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

Data Provider P_i $(i \in [1, k])$ does:;
Initialize the Models parameters randomly;
Sample a key tuple:$(pk_i, sk_i, ek_i) \leftarrow KeyGen(1^k)$;
Encrypt private data objects: m_i $W_i^{(j)}$ $\psi_i \leftarrow pub(m_i)||Enc(pk_i, sec(m_i))$ $d_i \leftarrow Enc(pk_i, W_i^{(j)})$, $g \leftarrow Enc(pk_i, t_i)$;
Crowdsource the private data to Data Service Provider:$(pk_i, ek_i, \psi_1, d_i, g_i)$;
Data Service Provider: $Enc(\mathcal{X}) \triangleq \{\langle pk_i, \psi_i \rangle\}$ an encrypted database which is the aggregation of public keys and ciphertext tuples. Execute *Algorithm 2* and *3* over the ciphertext domain;
Update the encrypted parameters: $\phi = \{W^1, W^2, b^1, b^2\}$;;
Send the learning results γ^* to the Data providers:;
The Data providers $P_i, P_2, \cdots, P_k$ do:;
The Data providers $P_i, P_2, \cdots, P_k$ jointly run a secure multiparty protocols to calculate ;
Evaluate$(\mathcal{C}), \{\langle pk_i, \psi_i \rangle\}$

In this paper, our proposed S-PPOC scheme will allow multiple data providers to outsource fully homomorphic ciphertext to a computational evaluator CE for storage and privacy-preserving data processing. Data Providers encrypt their datasets with different fully homomorphic encryption schemes to preserve the confidentiality of the private data. The application of the S-PPOC scheme involves the use of CSP and CE to collaboratively train a classification model over the datasets from these different entities. This classification model is stored in the encrypted form in CE. Which will be used to provide query response services for the Data Requestors.

7 Performance Evaluation

Our prototype is implemented in PySEAL [44]. PySEAL is python wrapper for the Microsoft Research's homomorphic encryption implementation, the Simple Encrypted Arithmetic Library (SEAL) homomorphic encryption library. The implementation of our privacy-preserving deep learning training model and classification were conducted on a computer NVIDIA GeForce GTX 780M 4096 MB @ 3.4 GHz, Intel Core i5 and 16 GB 1600 MHz DDR3 RAM and installed with Ubuntu Server 16.04 64-Bit Version.

7.1 Datasets

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

SBHARPT: SBHARPT [1, 37] is publicly available at [36]. The human activity recognition signals are generated with smartphones with embedded triaxial accelerometer and gyroscope. This devices are placed on the waist and with a constant frequency rate of 50Hz to collect 12 different kinds of activity signals such as walking, walking downstairs, walking upstairs, sitting, standing and laying. and 6 possible activity transitions: stand-to- sit, sit-to-lie, lie-to-sit, sit-to-stand, lie-to-stand and stand-to-lie. There are 815,614 records of sensor data.

OPPORTUNITY: Dataset from the opportunity [38] activity recognition is a composition of atomic activities generated with a sensor-based environment in excess of 27,000. Opportunity dataset comprises of recordings of 12 subjects with the application of 15 networked sensor systems with 72 sensors of 10 modalities, integrated into the WBAN attached to the human body. This experiment we consider the sensors on the body, which include initial measurement units and 3-axis accelerometer. Each of the sensor channels are therefore treated as an individual channels with a total of 113 channels. Opportunity dataset captures different postures and gestures whiles ignoring the null class. This is a composition of 18-class classification problem.

PAMAP2: PAMAP2 [35] physical activity monitoring dataset contains based on 18 different physical activities such as cycling, walking, Nordic walk, dancing, lie, sit, stand, run, iron, vacuum clean, rope jump, ascend and descend stairs, playing soccer were recorded from 9 participants (1 female and 8 males). In addition, a variety of leisure activities such as computer work, fold laundry, watch TV, drive car, clean house. The gyroscope, Accelerometer, magnetometer, temperature and heart rate data were recorded by 9 subjects wearing 3 inertial measurement unit with a heart rate monitor. The 3 calibre wireless inertial measurement units (IMU) with a sampling frequency of 100Hz: 1 IMU is placed over the wrist on the dominant arm, 1 IMU on the chest, and 1 IMU also on the dominant side of the ankle. The HR-monitor with a sampling frequency of 9Hz is therefore used to monitor the system over 10 hours.

7.2 Comparison Evaluation

In this section, with the consideration of privacy-preserving of human activity recognition applications, we apply our proposed S-PPOC model on the above mentioned public datasets. We compare our result with existing privacy-preserving deep neural network models and classifiers in terms of communication overhead and computational cost. The existing approaches are also based

on secure multi-party computations and fully homomorphic encryption.

Recently proposed schemes based on secure multiparty computations algorithm are [31] and [11]. Mohassel *et al.* presented SecureML which enables data providers distribute the private data among the two non-colluding servers in a distributed setting therefore falling under the two-server model where diverse neural network models are evaluated on the collaborative data using secure two-party computation. The authors use Yao's Garbled Circuit to securely perform deep learning. Two of the most important advantages of this setting are that,

1) Data owners can distribute their data inputs among the two non-colluding servers in the setup phase without engaging in any future computations.

2) It also benefit from a combination of efficient methods for Boolean computations such as the garbled circuits and oblivious Transfer extension and arithmetic computations.

They perform experiments on Arcene and MNIST datasets and report the results. As presented in Table 3 and Figure 3, S-PPOC significantly outperforms [31] and [11] in all aspects. It is important to note that, [26] decided to keep the computational cost and the communication cost of the data providers at a minimal level. The proposed algorithm classifies one instance at each prediction round. S-PPOC on the other hand is capable of classifying a bath of instances in each round with size 6152MB or larger.

To provide a fair comparison, we implemented the deep neural network with 2 hidden layers with 128 neurons in each of the layers without any convolutional layers using S-PPOC. In a 100 instances they reported 16 seconds as their running time whiles S-PPOC reported 10 seconds. By increasing the input batch size, the running time increases sub-linearly in [31] and [11] whereas in S-PPOC, the running time remains the same even when the input batch size becomes larger. Furthermore, S-PPOC does not require any communication between data providers and the cloud server for the provision of privacy-preserving predictions.

Table 3: Comparison with the state-of-the-art framework

Models	SBHARPT	PAMAP2	OPPORTUNITY
[31]	0.863	0.87	0.84
[11]	0.915	0.906	0.901
[26]	0.920	0.916	0.922
S-PPOC	0.954	0.935	0.955

Generally, existing secure multi-party deep learning privacy-preserving solutions have one of the biggest communication overheads since such schemes requires an interaction between the data providers and cloud server for the secure computations. [31] has a huge communication cost of 595.55MB for a relatively small convolutional neural network where as S-PPOC is only 257.4MB for the same work. Note that since the data providers participate in the training of the model and the computations, information about the deep neural network model may possibly be compromised. For example, the data providers can learn information such as the structure of the layers, activation functions and the number of the layers therefore demonstrating the potential for security breaches.

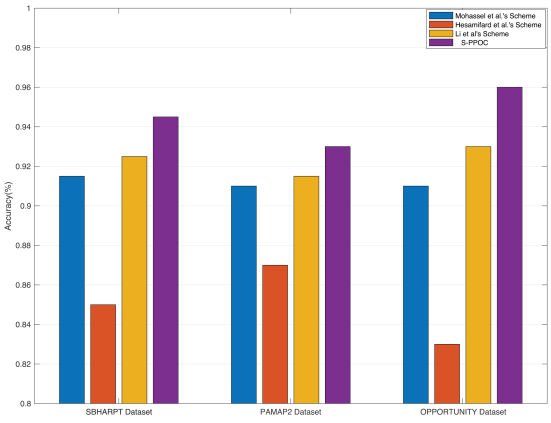

Figure 3: Performance comparison of S-PPOC with state-of-the-arts models on public datasets

8 Conclusion and Future Work

In this paper, we propose a S-PPOC scheme will allows multiple human activity recognition data providers to outsource fully homomorphic ciphertext to a computational evaluator CE for storage and privacy-preserving data processing. Data Providers encrypt their datasets with different fully homomorphic encryption schemes to preserve the confidentiality of the private data. The application of the S-PPOC scheme involves the use of CSP and CE to collaboratively train a classification model over the datasets from these different entities. This classification model is stored in the encrypted form in CE. Which will be used to provide query response services for the Data Requestors.

Acknowledgments

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] D. Anguita, A. Ghio, L. Oneto, X. Parra, and J. L. Reyes-Ortiz, "A public domain dataset for human activity recognition using smartphones," in *The 21st European Symposium on Artificial Neural Networks*, 2013. (https://www.elen.ucl.ac.be/Proceedings/esann/esannpdf/es2013-84.pdf)

[2] A. Bansal, T. Chen, and S. Zhong, "Privacy preserving back-propagation neural network learning over arbitrarily partitioned data," *Neural Computing and Applications*, vol. 20, no. 1, pp. 143–150, 2011.

[3] Z. Brakerski, C. Gentry, and V. Vaikuntanathan, "(leveled) fully homomorphic encryption without bootstrapping," *ACM Transactions on Computation Theory*, vol. 6, no. 3, pp. 13:1–13:36, 2014.

[4] D. Chen, N. Zhang, N. Cheng, K. Zhang, Z. Qin, and X. S. Shen, "Physical layer based message authentication with secure channel codes," *IEEE Transactions on Dependable and Secure Computing*, vol. 17, no. 5, pp. 1079–1093, 2018.

[5] D. Chen, N. Zhang, R. Lu, N. Cheng, K. Zhang, and Z. Qin, "Channel precoding based message authentication in wireless networks: Challenges and solutions," *IEEE Network*, vol. 33, no. 1, pp. 99–105, 2018.

[6] D. Chen, N. Zhang, R. Lu, X. Fang, K. Zhang, Z. Qin, and X. Shen, "An LDPC code based physical layer message authentication scheme with prefect security," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 4, pp. 748–761, 2018.

[7] D. Chen, N. Zhang, Z. Qin, X. F. Mao, Z. Qin, X. Shen, and X. Y. Li, "S2M: A lightweight acoustic fingerprints-based wireless device authentication protocol," *IEEE Internet of Things Journal*, vol. 4, no. 1, pp. 88–100, 2017.

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

[9] R. Gilad-Bachrach, N. Dowlin, K. Laine, K. E. Lauter, M. Naehrig, and J. Wernsing, "Cryptonets: Applying neural networks to encrypted data with high throughput and accuracy," in *Proceedings of the 33nd International Conference on Machine Learning*, vol. 48, pp. 201–210, 2016.

[10] S. Gong, B. B. Yin, Z. Zheng, and K. Y. Cai, "Adaptive multivariable control for multiple resource allocation of service-based systems in cloud computing," *IEEE Access*, vol. 7, pp. 13817–13831, 2019.

[11] E. Hesamifard, H. Takabi, and M. Ghasemi, "Cryptodl: Deep neural networks over encrypted data," *CoRR*, vol. abs/1711.05189, 2017.

[12] Y. L. Hsu, S. C. Yang, H. C. Chang, and H. C. Lai, "Human daily and sport activity recognition using a wearable inertial sensor network," *IEEE Access*, vol. 6, pp. 31715–31728, 2018.

[13] H. Hui, X. Li, and Y. Sun, "A triboelectric motion sensor in wearable body sensor network for human activity recognition," in *The 38th Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, pp. 4889–4892, 2016.

[14] S. Ioffe and C. Szegedy, "Batch normalization: Accelerating deep network training by reducing internal covariate shift," in *Proceedings of the 32nd International Conference on Machine Learning*, vol. 37, pp. 448–456, 2015.

[15] A. N. Jaber, Z. M. Fadli, and H. Othman, "A conceptual model using the elliptic curve Diffie-Hellman with an artificial neural network over cloud computing," *The National Conference for Postgraduate Research*, 2016. (https://www.researchgate.net/publication/308548189_A_Conceptual_Model_Using_the_Elliptic_Curve_Diffie-Hellman_With_An_Artificial_Neural_Network_Over_Cloud_Computing)

[16] A. N. Jaber and M. F. B. Zolkipli, "Use of cryptography in cloud computing," in *IEEE International Conference on Control System, Computing and Engineering*, pp. 179–184, 2013.

[17] S. Kim, S. Yeom, O. J. Kwon, D. Shin, and D. Shin, "Ubiquitous healthcare system for analysis of chronic patients' biological and lifelog data," *IEEE Access*, vol. 6, pp. 8909–8915, 2018.

[18] O. A. Kwabena, Z. Qin, T. Zhuang, and Z. Qin, "Mscryptonet: Multi-scheme privacy-preserving deep learning in cloud computing," *IEEE Access*, vol. 7, pp. 29344–29354, 2019.

[19] C. Lai, H. Li, R. Lu, and X.(Sherman) Shen, "SE-AKA: A secure and efficient group authentication and key agreement protocol for LTE networks," *Computer Networks*, vol. 57, no. 17, pp. 3492–3510, 2013.

[20] C. T. Li, M. S. Hwang, "A lightweight anonymous routing protocol without public key en/decryptions for wireless ad hoc networks",*Information Sciences*, vol. 181, no. 23, pp. 5333–5347, Dec. 2011.

[21] C. T. Li, M. S. Hwang, Y. P. Chu, "Further improvement on a novel privacy preserving authentication and access control scheme for pervasive computing environments", *Computer Communications*, vol. 31, no. 18, pp. 4255–4258, Dec. 2008.

[22] C. T. Li, M. S. Hwang, Y. P. Chu, "A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks", *Computer Communications*, vol. 31, no. 12, pp. 2803-2814, July 2008.

[23] C. T. Li, M. S. Hwang and Y. P. Chu, "An efficient sensor-to-sensor authenticated path-key establishment scheme for secure communications in wireless sensor networks", *International Journal of Innovative Computing, Information and Control*, vol. 5, no. 8, pp. 2107-2124, Aug. 2009.

[24] J. Li, L. Tian, H. Wang, Y. An, K. Wang, and L. Yu, "Segmentation and recognition of basic and transi-

tional activities for continuous physical human activity," *IEEE Access*, vol. 7, pp. 42565–42576, 2019.

[25] P. Li, J. Li, Z. Huang, T. Li, C. Z. Gao, S. M. Yiu, and K. Chen, "Multi-key privacy-preserving deep learning in cloud computing," *Future Generation Computer Systems*, vol. 74, pp. 76–85, 2017.

[26] T. Li, Z. Huang, P. Li, Z. Liu, and C. Jia, "Outsourced privacy-preserving classification service over encrypted data," *Journal of Network and Computer Applications*, vol. 106, pp. 100–110, 2018.

[27] Z. Li and T. H. Lai, "On evaluating circuits with inputs encrypted by different fully homomorphic encryption schemes," *IACR Cryptology ePrint Archive*, vol. 2013, p. 198, 2013.

[28] C. H. Ling, C. C. Lee, C. C. Yang, and M. S. Hwang, "A secure and efficient one-time password authentication scheme for WSN", *International Journal of Network Security*, vol. 19, no. 2, pp. 177-181, Mar. 2017.

[29] L. H. Liu and Y. Liu, "A note on one outsourcing scheme for large-scale convex separable programming," *International Journal of Electronics and Information Engineering*, vol. 12, no. 4, pp. 155-161, 2020.

[30] A. López-Alt, E. Tromer, and V. Vaikuntanathan, "On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption," in *Proceedings of the 44th Symposium on Theory of Computing Conference*, pp. 1219–1234, 2012.

[31] P. Mohassel and Y. Zhang, "Secureml: A system for scalable privacy-preserving machine learning," in *IEEE Symposium on Security and Privacy*, 2017. (`https://eprint.iacr.org/2017/396.pdf`)

[32] T. Muhammed, R. Mehmood, A. Albeshri, and I. Katib, "Ubehealth: A personalized ubiquitous cloud and edge-enabled networked healthcare system for smart cities," *IEEE Access*, vol. 6, pp. 32258–32285, 2018.

[33] Z. Qin, L. Hu, N. Zhang, D. Chen, K. Zhang, Z. Qin, and K. K. R. Choo, "Learning-aided user identification using smartphone sensors for smart homes," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 7760–7772, 2019.

[34] Z. Qin, Y. Wang, H. Cheng, Y. Zhou, Z. Sheng, and V. C. M. Leung, "Demographic information prediction: A portrait of smartphone application users," *IEEE Transactions on Emerging Topics in Computing*, vol. 6, no. 3, pp. 432–444, 2018.

[35] A. Reiss and D. Stricker, "Introducing a new benchmarked dataset for activity monitoring," in *The 16th International Symposium on Wearable Computers*, pp. 108–109, 2012.

[36] J. L. Reyes-Ortiz, D. Anguita, L. Oneto and X. Parra, *Smartphone-Based Recognition of Human Activities and Postural Transitions Data Set*, 2015. (`https://archive.ics.uci.edu/ml/datasets/Smartphone-Based+Recognition+of+Human+Activities+and+Postural+Transitions`)

[37] J. L. Reyes-Ortiz, L. Oneto, A. Ghio, A. Samà, D. Anguita, and X. Parra, "Human activity recognition on smartphones with awareness of basic activities and postural transitions," in *International Conference on Artificial Neural Networks (ICANN'14)*, vol. 8681, pp. 177–184, 2014.

[38] D. Roggen, A. Calatroni, M. Rossi, T. Holleczek, K. Förster, G. Tröster, P. Lukowicz, D. Bannach, G. Pirkl, A. Ferscha, J. Doppler, C. Holzmann, M. Kurz, G. Holl, R. Chavarriaga, H. Sagha, H. Bayati, M. Creatura, and J. del R. Millán, "Collecting complex activity datasets in highly rich networked sensor environments," in *Seventh International Conference on Networked Sensing Systems*, pp. 233–240, 2010.

[39] H. Saleh, H. Nashaat, W. Saber, and H. M. Harb, "IPSO task scheduling algorithm for large scale data in cloud computing environment," *IEEE Access*, vol. 7, pp. 5412–5420, 2019.

[40] S. Shen, J. Qian, D. Cheng, K. Yang, and G. Zhang, "A sum-utility maximization approach for fairness resource allocation in wireless powered body area networks," *IEEE Access*, vol. 7, pp. 20014–20022, 2019.

[41] S. Sodagari, B. Bozorgchami, and H. Aghvami, "Technologies and challenges for cognitive radio enabled medical wireless body area networks," *IEEE Access*, vol. 6, pp. 29567–29586, 2018.

[42] D. Stehlé and R. Steinfeld, "Faster fully homomorphic encryption," in *International Conference on the Theory and Application of Cryptology and Information Security*, vol. 6477, pp. 377–394, 2010.

[43] H. Takabi, E. Hesamifard, and M. Ghasemi, "Privacy Preserving Multi-party Machine Learning with Homomorphic Encryption," *Proceedings of the Workshop on Private Multi-Party Machine Learning*, no. Nips, pp. 1–5, 2016.

[44] A. J. Titus, S. Kishore, T. Stavish, S. M. Rogers, and K. Ni, "Pyseal: A python wrapper implementation of the SEAL homomorphic encryption library," *CoRR*, vol. abs/1803.01891, 2018.

[45] H. Xiong, H. Zhang, and J. Sun, "Attribute-based privacy-preserving data sharing for dynamic groups in cloud computing," *IEEE Systems Journal*, vol. 13, no. 3, pp. 2739–2750, 2019.

[46] C. Yang, Q. Chen, Y. Liu, "Fine-grained outsourced data deletion scheme in cloud computing," *International Journal of Electronics and Information Engineering*, vol. 11, no. 2, pp. 81–98, 2019.

[47] J. Yuan and S. Yu, "Privacy preserving back-propagation neural network learning made practical with cloud computing," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 1, pp. 212–221, 2014.

[48] N. Zhang, P. Yang, J. Ren, D. Chen, L. Yu, and X. Shen, "Synergy of big data and 5g wireless networks: Opportunities, approaches, and challenges," *IEEE Wireless Communications*, vol. 25, no. 1, pp. 12–18, 2018.

[49] N. Zhang, P. Yang, S. Zhang, D. Chen, W. Zhuang, B. Liang, and X. S. Shen, "Software defined networking enabled wireless network virtualization: Challenges and solutions," *IEEE Network*, vol. 31, no. 5, pp. 42–49, 2017.

[50] Q. Zhang, L. T. Yang, Z. Chen, P. Li, and M. J. Deen, "Privacy-preserving double-projection deep computation model with crowdsourcing on cloud for big data feature learning," *IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 2896–2903, 2018.

[51] H. Zhu, R. Lu, X. Shen, and X. Lin, "Security in service-oriented vehicular networks," *IEEE Wireless Communications*, vol. 16, no. 4, pp. 16–22, 2009.

Biography

Owusu-Agyemang Kwabena is currently a Ph. D. candidate in the School of Information and Software Engineering, University of Electronic Science and Technology of China (UESTC). He received his MSc. degree from Coventry University in 2012. His research interests include machine learning, data mining, big data analysis, applied cryptography, blockchain technology and medical image processing.

Zhen Qin is currently an associate professor in the School of Information and Software Engineering, University of Electronic Science and Technology of China (UESTC). He received his Ph.D. degree from UESTC in 2012. He was a visiting scholar in the Department of Electrical Engineering and Computer Science at Northwestern University. His research interests include network measurement, mobile social networks, wireless sensor networks and medical image processing.

Hu Xiong received the Ph.D. degree from the School of Computer Science and Engineering, University of Electronic Science and Technology of China (UESTC) in 2009. He is currently a Full Professor with the School of Information and Software Engineering, UESTC. His research interests include applied cryptography and cypberspace security. He is a member of IEEE.

Yao Liu is currently an associate professor in the School of Information and Software Engineering, University of Electronic Science and Technology of China (UESTC). She received her Ph.D. degree from UESTC in 2016. Her research interests include machine learning, social networks, network security and data mining.

Tianming Zhuang is currently an undergraduate in Glasgow College, University of Electronic Science and Technology of China (UESTC). His research interests include big data analysis and data mining.

Zhiguang Qin is the full professor of the School of Information and Software Engineering in University of Electronic Science and Technology of China (UESTC), where he is also Director of the Key Laboratory of New Computer Application Technology and Director of UESTC-IBM Technology Center. His research interests include medical image processing, computer networking, information security, cryptography, information management, intelligent traffic, electronic commerce, distribution, and middleware.