Private Facial Prediagnosis as an Edge Service for Parkinson's DBS Treatment Valuation

Richard Jiang, Paul Chazot, Nicola Pavese, Danny Crookes, Ahmed Bouridane, and M. Emre Celebi

***Abstract*—Facial phenotyping for medical prediagnosis has recently been successfully exploited as a novel way for the preclinical assessment of a range of rare genetic diseases, where facial biometrics is revealed to have rich links to underlying genetic or medical causes. In this paper, we aim to extend this facial prediagnosis technology for a more general disease, Parkinson's Diseases (PD), and proposed an Artificial-Intelligence-of-Things (AIoT) edge-oriented privacy-preserving facial prediagnosis framework to analyze the treatment of Deep Brain Stimulation (DBS) on PD patients. In the proposed framework, a novel edge-based privacy-preserving framework is proposed to implement private deep facial diagnosis as a service over an AIoT-oriented *information theoretically secure* multi-party communication scheme, while data privacy has been a primary concern toward a wider exploitation of Electronic Health and Medical Records (EHR/EMR) over cloud-based medical services. In our experiments with a collected facial dataset from PD patients, for the first time, we proved that facial patterns could be used to evaluate the facial difference of PD patients undergoing DBS treatment. We further implemented a privacy-preserving information theoretical secure deep facial prediagnosis framework that can achieve the same accuracy as the non-encrypted one, showing the potential of our facial prediagnosis as a trustworthy edge service for grading the severity of PD in patients.**

***Index Terms*—Edge AIoT, electronic health and medical records, facial prediagnosis, medical biometrics, private deep learning, private biometrics.**

Manuscript received May 21, 2021; revised December 16, 2021; accepted January 9, 2022. Date of publication January 27, 2022; date of current version June 6, 2022. This work was supported in part by the U.K. EPSRC under Grant EP/P009727/1, in part by the Leverhulme Trust under Grant RF-2019-492, and in part by the U.S. National Science Foundation under Grant 1946391. *(Correspondent author: Richard Jiang.)*

Richard Jiang is with the Lancaster University, LA1 4YW Lancaster, U.K. (e-mail: panperception@outlook.com).

Paul Chazot is with the School of Biosciences, Durham University, DH1 3DE Durham, U.K. (e-mail: paul.chazot@durham.ac.uk).

Nicola Pavese is with the NHS Clinical Ageing Research Unit, Newcastle University, NE4 5PL Newcastle upon Tyne, U.K. (e-mail: nicola.pavese@newcastle.ac.uk).

Danny Crookes is with the School of Electronics, Electrical Engineering and Computer Science, Queen's University Belfast, BT3 9DT Belfast, U.K. (e-mail: d.crookes@qub.ac.uk).

Ahmed Bouridane was with the Northumbria University, NE1 8ST Newcastle upon Tyne, U.K. He is now with the Center for Data Analytics and Cybersecurity, University of Sharjah, Sharjah 27272, UAE (e-mail: abouridane@sharjah.ac.ae).

M. Emre Celebi is with the Department of Computer Science and Engineering, University of Central Arkansas, Conway, AR 72035 USA (e-mail: ecelebi@uca.edu).

Digital Object Identifier 10.1109/JBHI.2022.3146369

I. Introduction

FACIAL diagnosis dates back to 2000 years ago in Traditional Chinese Medicine (TCM) practice [1], [2]. Recently, scientists have shown that facial phenotyping [3]–[8] can be used to diagnose accurately over 200 rare genetic diseases, reviving this ancient technology as a new method potentially for diagnosing a wide range of diseases. In addition to applying to rare diseases, facial prediagnosis may have a potential to be applied to many common illnesses. In this paper, we will look into the quantifiable modelling on facial prediagnosis of Parkinson's disease (PD) [9]–[14], while it has been widely reported that PD has an apparent impact on the faces of PD patients, like many other neurodegenerative diseases [11], [12].

PD can affect natural facial expressions in addition to gross motor skills. This phenomenon, called "facial-masking" (hypomimia) [12], is a common sign of early PD, arising prior to major motor and non-motor symptoms. This is due to a reduction of automatic and controlled expressive movement of facial musculature, creating an appearance of apathy, social disengagement or compromised cognitive status. Such facial symptoms can have significant negative effects on mental health, as it distorts the perceived emotional responses of the individual [11], which can lead to misinterpretation by friends, family and the public. Hence, via facial diagnosis, we can expect that a robust computational model can capture subtle variations of facial features, establish quantifiable evidence and measure/predict the developmental stages of Parkinson's Diseases.

Unlike other senescent diseases, PD is featured by two distinct issues [10]. First, there is no cure for Parkinson's diseases. However, early detection can help the adoption of an early intervention to slow down the PD progress. Second, there is no test for Parkinson's diagnosis, making it hard to identify PD at its early stages. Though we can find evidences from EEG or MRI scanning at a developed stage, it is often too late. Instead, Parkinson's diagnosis [10] is often based on the examination by a well-trained expert on tremor at rest, rigidity, slowness and loss of spontaneous movement, a characteristic way of walking, a frozen smile on face, etc. While such visually observable symptoms can be captured by AI-powered video-based facial analysis, in this work, to save the precious time of doctors,

Fig. 1. Facial images of a PD patient before and after Deep Brain Stimulation treatment.

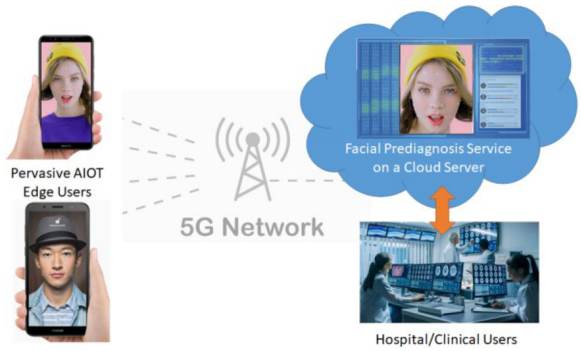


Fig. 2. Facial Prediagnosis over 5G AIoT edge service.

nurses and care staff from examining mass communities, we aim to develop AI-based facial diagnosis for PD.

Parkinson's Diseases [9]–[14] is a heterogeneous disease (no case being exactly the same), with motor symptoms including tremor, rigidity, bradykinesia, dyskinesia (drug-induced), and non-motor symptoms, including dementia, anxiety, depression, sleep dysfunction, psychosis, persistent pain, delirium, gambling compulsion etc. At the early developmental stage, these symptoms are subtle and occasional. Via automated facial diagnosis, individuals in a range of settings can be monitored and diagnosed quickly and scored on the risk of potential phenotypes of PDs for doctors/caregivers to consider social interventions and palliative therapies. Facial diagnosis [1]–[8] can provide a cost-effective staff-free automated diagnosis platform via 24/7 real-time online surveillance of patients in care with no waiting time. Potentially, it will enable early diagnosis for preventive treatments over a large population in care and help provide accurate phenotyping for timely precision medicine or treatment. To enable facial prediagnosis for PD analysis, there are two challenges that need to overcome:

1) First, we need proof-of-concept experiments to show that facial images can be practically used to classify PD patients with suitable accuracy.
2) Secondly, due to privacy issues, the facial biometrics of patients need to be restricted to private use instead of circulating over Internet servers, and a privacy-preserved framework is needed for automated facial diagnosis services over cloud-based networks.

In this paper, taking the PD treatment via Deep Brain Stimulation (DBS) as our case study, we aim to develop a private IoT-based facial prediagnosis framework to evaluate the facial difference of DBS treatment on patients by comparing facial biometrics before and after DBS.

Fig. 1 shows the sample facial images of a patient before and after DBS treatment, respectively. Facial images are deformable, and key features are subtle to discriminate. Cross-subject classification becomes more challenging particularly, when the training dataset consists of totally different subjects from the test dataset. Although there are reports that links facial features to PDs [11], [12], up to now it has not been certain if we can use facial images to grade the severity of PD patients via machine learning. In this paper, we will prove this concept using a deep learning based framework.

The scenario of cloud-based automated facial prediagnosis can be depicted in Fig. 2. The face photo of a patient can be collected at an Artificial-Intelligence-of-Thing (AIoT) edge device such as a mobile phone, and the face photo is then sent to the server of the service provider. Due to privacy concerns and legislation, patients (or hospitals) may not allow their electronic health or medical records (EHR or EMR) to upload to a server in an external business. Hence, a privacy-aware framework is then required for the purpose of commercialized facial diagnosis services to offer a widely accessible platform for point-of-care (POC) AIoT end users.

To address the privacy issue in medical prediagnosis, it has been reported to utilize Partial Homomorphic Encryption(PHE) to implement privacy-preserving algorithms such as Support Vector Machine[19] or Naïve Bayesian Classification[15]. However, the implementation of deep neural networks (DNNs) via PHE is yet not applied to medical prediagnosis, while DNNs have nonlinear activation functions that cannot be directly mapped to the encryption domain.

In our proposed solution, we will aim to exploit the multi-party communication architecture and propose an information theoretical secure framework for privacy-preserving deep learning based facial prediagnosis. Our novel contributions in this work include three key aspects, as detailed below:

1) *A novel PD prediagnosis method*: Our work presents a novel preclinical assessment method on PD via facial prediagnosis that achieved good accuracy in our experiments, implying a great value of facial prediagnosis for further exploitation on medical purposes.
2) *Novel information-theoretical secure implementation*: We implemented a novel AIoT-based framework for privacy-preserving deep learning based facial diagnosis, which is information theoretical secure and achieved the equivalent accuracy in comparison with the original non-privacy-preserving facial diagnosis algorithm.
3) *Clinical trial*: we present our experiments with 52 PD patients before and after Deep Brain Stimulation (DBS), which offers a valuable medical trial from our report.

We implemented our initial demo with a PHE library and validated our implementation as the proof-of-concept on a video datasets of 52 PD patients who received the DBS treatments. Our experiments show an accuracy over 95% on discriminating facial features before and after treatment. In comparison, it was reported EEG-based prediagnosis [45] has an accuracy of 85%.

TABLE I
COMPARISON OF FHE AND PHE ALGORITHMS

Ops.	FHE			PHE		
	SEAL	HElib	TFHE	Pallier	ELGamal	RSA
Add/Sub	√	√	√	√	×	×
Multiply	√	√	√	×	√	√
Division	×	×	×	×	×	×
Compare	×	×	×	×	×	×
Matrx Ops	√	√	×	×	×	×
Exp	√	√	×	×	×	×
Square	√	√	√	×	√	√
Negation	√	√	×	×	×	×

The remainder of the paper is organized as follows. Section 2 reviews the existing relevant work. Section 3 gives background on PHE and describes its implementation. Section 4 presents the proposed AIoT-based privacy-preserving deep learning framework. Section V shows the experimental results. Finally, Section VI concludes the paper.

II. PRELIMINARY ON PRIVATE MACHINE LEARNING

To protect the privacy of shared data over the Internet, it has been widely researched to use various encryption methods [15]–[30] to secure the data under various hostile or curious conditions. While privacy can be mostly assured by a sophisticated encryption scheme, the data services that need to carry out various computations on the data cannot work due to the encryption. To solve this issue, homomorphic encryption schemes have become a popular way to protect the private data while enabling computation, such as machine learning, to operate on encrypted data.

Partial Homomorphic Encryption, as its name suggests, can maintain only some homomorphic features in its encryption, while full homomorphic encryption is expected to be able to carry out all equivalation arithmetic operations in its encrypted domain. Typical PHE algorithms include Pallier, ELGamel, and RSA [21]. Well known FHE libraries include SEAL, HElib and TFHE [20]. Table I gives a comparison of several existing open encryption algorithms. We can see that division and comparison are not yet available in PHE or FHE algorithms. Unlike FHE algorithms, PHE algorithms cannot support bitwise operation, exponentiation, negation, and add/subtract with plain texts.

Although PHE does not provide all operations to implement deep learning in the encrypted domain, in this paper, we will demonstrate a new scheme to fulfill the privacy-preserving deep learning without resorting to expensive FHE ones. By taking the Pallier cryptosystem as our encryption method, we will show a full implementation of privacy-preserving deep neural networks using PHE based on an AIoT framework. The reasons for choosing PHE instead of Full Homomorphic Encryption (FHE) include: 1) PHE has been applied for medical applications for years [15∼19] and is relatively mature with much lower costs; 2) It is less compute-intensive than full homomorphic encryption (FHE) [19]–[21] and thus easier to deploy on AIoT devices; 3) PHE based machine learning has recently been successfully utilized on facial images [22]–[25]. Hence, a PHE based privacy-preserving deep learning framework is a rational choice for our facial prediagnosis application.

There have been a number of reported applications of privacy-preserving machine learning [15]–[30]. The majority of these are developed for distributed setting where different parties hold parts of the training database and securely train a common classifier without each party needing to disclose its own training data to other parties. Recently, Pallier encryption has been applied successfully for facial classification using classic linear machine learning methods [22]–[25] such as SVM, LDA, etc. In our work, we aim to utilize deep learning for our facial diagnosis service, because deep learning has achieved greater robustness and better accuracy in pattern classification [3], [6]–[8].

There have been reports of various FHE based deep learning implementations [20], [31]–[35]. However, it is yet challenging to implement the nonlinear functions in neurons since FHE is fundamentally based on linearization lattice. As shown in Table I, current FHE methods cannot yet cope with divide and compare [20]. Its implementation of exponention is based on the repeating squaring algorithm, which causes extra computational complexity and accuracy concerns, and can be applied only to positive number exponentiation [20]. Due to the complexity, most reported implementations assumes the linear approximation of nonlinear functions, with no guarantee of the control of extra errors [29]–[33]. On the other side, PHE is relatively less compute-intensive [22]–[24]. Hence, in our application to PD, we choose PHE to implement a lightweight framework for privacy-preserving deep learning.

While the current trend is to provide AI-enabled medical diagnosis as a service [15], [16], [18], [19], [21], the needs to preserve the privacy of the data comes with data sharing over distributed systems, cloud-based services, 5G/6G communication, Internet-of-Things, etc. There are many reported frameworks to try to meet the various needs. In [29], the encrypted data from clients are decrypted on the server side before feeding into the deep neural networks and the final results are encrypted before sending back to clients. However, this implies the server can know the client's private data with no privacy protection, though it may be secure to third parties in the communication nodes. In [33], the encryption is performed partially on the layers of deep neural networks. However, asymmetric encryption, although data is hidden from each other, lacks robustness due to the exposure of public keys, leaving it vulnerable if sufficient attempts are made, particularly when the emerging quantum computing becomes available [36]–[38]. Hence, these proposed schemes over multi-party communication will not be secure in the information theoretical sense.

In this work, we are concerned with facial diagnosis over AIoT services. When patients or hospitals send their data over to the commercial service provider, they may not want to risk compromising the privacy of their patients. On the other side, the service provider wants to keep their learned model safe, and does not want to be exposed to an end user. Hence an information theoretically secure scheme is required for such automated medical data services.

Encrypted facial recognition has been implemented with many algorithms [22]–[25]. Privacy-preserving data classification algorithms suitable for a client-server model were studied in [39]–[41]. The client-server model substantially reduces the computational and communication overhead at the client since it needs to interact with only one server compared to a more distributed setting. Outsourcing the clinical decision support system to a third-party server without violating the client's privacy was studied in [15]–[19], [21]–[24], [28]–[35].

In this paper, in contrast to these previous works, we propose a lightweight privacy-preserving medical diagnosis protocol based on encrypted deep learning over an information theoretically secured AIoT framework. We will demonstrate that our proposed facial diagnosis framework achieves the desired privacy requirements without degrading the classification performance, and the computational and communication complexity are under control.

III. Privacy-Preserving DNN Implementation

Considering the scenario that AIoT users send their encrypted facial images to the automated medical diagnosis server hosted by a commercial service provider, we need to find a robust privacy-preserving scheme to guarantee data privacy in the system. To achieve this, as detailed in the above sections, we choose the Paillier cryptosystem as our encryption engine, which is partially homomorphic.

A. The Paillier Cryptosystem

Typical PHE algorithms [21]–[24] include Unpadded RSA, ElGamal encryption, Goldwasser–Micali cryptosystem, Benaloh cryptosystem, Paillier cryptosystem, etc. The Paillier cryptosystem [24] is an additive homomorphic encryption method. The Paillier cryptosystem, invented by and named after Pascal Paillier in 1999, is a probabilistic asymmetric algorithm for public key cryptography. The problem of computing n^{th} residue classes is known to be computationally difficult. The decisional composite residuosity assumption is the intractability hypothesis upon which this cryptosystem is based.

Like most other RSA-like algorithms, the Paillier encryption needs a pair of keys, namely public and private keys. The keys are generated via the process below:

1) Public keys: Choose two large prime numbers p and q randomly and independently of each other such that: $gcd(pq, (p-1)(q-1)) = 1$. Compute $n = pq$ and $\lambda = \text{lcm}(p\text{-}1, q\text{-}1)$.
2) Select a random integer $g \in Z^*_{n^2}$, and calculate the modular multiplicative inverse:

$$\mu = \text{mod}\left(\frac{n}{\text{mod}\left(g^{\lambda}, n^2\right) - 1}, n\right) \tag{1}$$

Here the division gives the integral quotient.

With the above two steps, the generated public keys are $\{n, g\}$ and the private keys are $\{\lambda, \mu\}$.

After keys are produced, the encryption step will be decided by public keys only. Assuming t is the message to encrypted and satisfies $0 \leq t < n$, and r is a random number and satisfies $0 \leq r < n$ and $r \in Z^*_n$, the cipher text can be obtained as:

$$c = [\![t|r]\!] = \text{mod}\left(g^t r^n, n^2\right) \ and \ c \in Z^*_{n^2} \tag{2}$$

Here, $*$ denotes the encryption. The random number r will make the Paillier encryption as non-deterministic. Every time with the same keys, the same text t will have different cipher text c.

Inversely, the decipher step will be based on the private keys, and

$$t = \langle c \rangle = \text{mod}\left(\frac{\text{mod}\left(c^{\lambda}, n^2\right) - 1}{n}\mu, n\right) \tag{3}$$

Here, $\langle * \rangle$ denotes decryption in this paper. As it can be seen pointed out by Paillier in 1999 [21], decryption here is "essentially one exponentiation modulo n^2".

B. Homomorphic Properties

A notable feature of the Paillier cryptosystem is its homomorphic properties along with its non-deterministic encryption. The Pallier encryption function is additively homomorphic, and the product of two ciphertexts will decrypt to the sum of their corresponding plaintexts,

$$[\![t_1 + t_2]\!] = \text{mod}\left([\![t_1|r_1]\!] \cdot [\![t_2|r]\!]_2, n^2\right) \tag{4}$$

With the above equation, we can easily obtain the sum of two encrypted numbers without deciphering them.

Besides the additive homomorphic property, the encrypted numbers in the Paillier cryptosystem can implement the negation homomorphic property as,

$$[\![t_1 \times t_2]\!] = \text{mod}\left([\![t_1]\!]^{t_2}, n^2\right) \tag{5}$$

Here, it is noted that t_2 must be in its original value. Given the Paillier encryptions of two messages there is no known way to compute an encryption of the product of these messages without knowing the private key.

Based on the above partial multiplicative homomorphic property, the encrypted numbers in the Pallier cryptosystem can implement a form of the negation homomorphic property,

$$[\![-t_1]\!] = \text{mod}\left([\![t_1]\!]^{-1}, n^2\right) \tag{6}$$

This is particularly useful since in artificial neurons we have negative weights and bias.

Sometimes we may need to add the ciphertext with a plain text, which could be done simply by,

$$[\![t_1]\!] + [\![t_2]\!] = t_1 + \text{mod}\left([\![1]\!]^{-t_2}, n^2\right) \tag{7}$$

Here, a plaintext is encoded by taking advantage of the ciphertext $[\![1]\!]$ and Eq. (5), without knowing the encryption keys (including public keys).

C. Encrypted Faces

Consider a pattern or image consisting of $W \times H$ pixels, where each pixel is represented by its intensity value x_i. Using Eq. [2], we can then obtain the encrypted big integer $z_i = [\![x_i]\!]$ for each pixel. Normalizing $\{z_i\}$ by n^2, we can obtain the whole

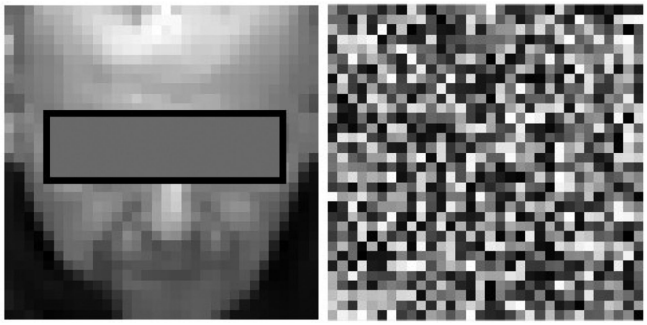


Fig. 3. Encrypted digital patterns.

encrypted images shown in Fig. 3. The original images are on the left, and the corresponding encrypted patterns are visualized on the right.

As we can observe from Fig. 3, the encrypted patterns are no longer visually identifiable, though each pattern contains exactly the same amount of information as the original images. However, without knowing the keys, no one can decipher the patterns. Hence, data security and privacy can be safely guaranteed, unlike other alternative arrangements in many private learning methods [15]–[19] that may compromise the security over shared keys between multiple parties.

D. Encrypted Neurons Without Keys

Artificial neurons are a simplified model of biological neurons that contain multiple synaptic inputs and one axon output. The model of an artificial neuron consists of a weighted-sum process that can be described as,

$$y_j = \sum_{i=1}^{K} w_i x_i \ + b_j \tag{8}$$

where x_i are the input signals and y_j is the summation result that will be capped by an activation process, typically the sigmoid function,

$$z_j = \frac{1}{1 - \mathrm{e}^{-y_j}} \tag{9}$$

z_j denotes the final output from the j-th neuron in a layer.

If we have encrypted inputs $[\![x_i]\!]$, then the addition process in the above neuron model will be described as,

$$\begin{aligned}[\![y_j]\!] &= \left[\!\left[\sum_{i=1}^{K} w_i x_i + b_j\right]\!\right] = mod\left(\left[\!\left[\sum_{i=1}^{K} w_i x_i\right]\!\right] \cdot [\![b_j]\!], n^2\right) \\ &= mod\left(\left(\prod_{i=1}^{K} [\![w_i x_i]\!]\right) \cdot [\![b_j]\!], n^2\right) \\ &= mod\left(\left(\prod_{i=1}^{K} [\![x_i]\!]^{w_i}\right) \cdot [\![b_j]\!], n^2\right)\end{aligned} \tag{10}$$

Hence, the calculation can be easily carried out directy on the encrypted inputs. Here, we may need to encrypt the bias value in the learned neuron model. To make it simple, we can take advantage of Eq. (5) and obtain,

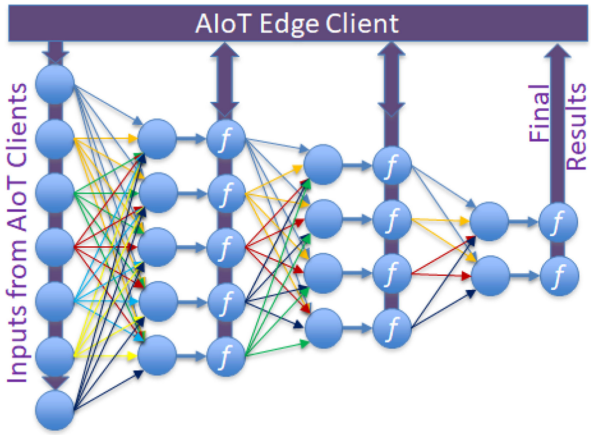


Fig. 4. An encryption based private deep neural network running in a server communicating with AIoT edge clients.

$$[\![b_j]\!] = [\![1 \times b_j]\!] \ = \ \mathrm{mod}\left([\![1]\!]^{b_j}, n^2\right) \tag{11}$$

Hence, we do not need any encryption keys to fulfil the above calculation if the big integer value of $[\![1]\!]$ is given.

The calculation of the activation function in Eq. (9) on encrypted data is a great challenge because it needs to carry out divisions and exponentiations in the encrypted domain. Some attempts adopting various linear approximation have been reported [34], [35]. However, these approximations may introduce unexpected errors. Similarly, the implementation of softmax functions on encrypted data suffers from similar difficulties.

In this paper, we provide an AIoT-based solution to this challenge in privacy-preserving deep learning. Fig. 4 shows its schematic view. While the learned model is stored in the server in a layer-wise structure, the activation functions are computed via queries to the AIoT clients in a distributed computing framework, and the computational load is shared by the server and the clients. More details can be found in the following section.

IV. AIoT-Based Information Theoretical Secure Deep Facial Diagnosis

With the PHE-enabled encrypted neurons, we can then implement a given neural network layer by layer. Details are described below, based on our proposed AIoT-oriented secure framework.

A. Overall Framework

The overall framework of our proposed AIoT-based facial diagnosis is detailed in the diagram in Fig. 5. The central medical service with well-trained deep neural networks resides on a cloud-based Honest-But-Curious (HBC) server, and AIoT edge clients can upload their encrypted data to the server. The encrypted data is then processed in a layer-wise mode through deep neural networks, and each layer is followed by the activation through the communication with the AIoT clients, as shown in the architecture in Fig. 4. The server

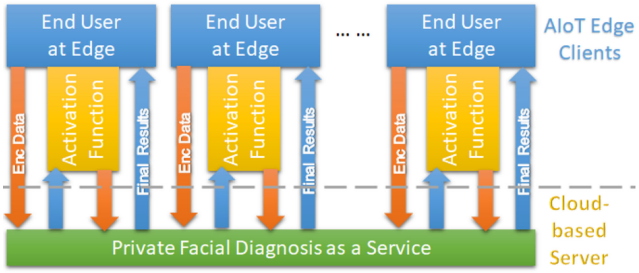


Fig. 5. Schematic view of the proposed privacy-protected client-server framework for AIoT edge services.

List I. Algorithms of the proposed framework.

Algorithm 1 AIoT Client

Inputs :

(1) Sample pair D_1 and D_2 for diagnosis
(2) Client ID *uid* and password *pwd*
(3) Server queries with *cmd* and *Xl*

Procedure :

setup bit length *Bl* and and float point length *Fl*
setup communication with server using *uid* and *pwd*
loop over D_1 & D_2:
create public & private keys of Pallier cryptosystem
encrypt D_k and 1, send to the diagnosis server
wait for the returned data from server: (*cmd, Xl*)
  if *cmd* is "sigmoid"
    calculate *sigm(* $\langle Xl \rangle$ *)*, encrypt & send to server
  if *cmd* is "softmax"
    calculate *softm(* $\langle Xl \rangle$ *)*, encrypt & send to server
  if *cmd* is "results"
    decrypt *Xl*, $R_k = \langle Xl \rangle$;
end loop
Compare the scores R_1 and R_2**:**
  if $R_1 > R_2$:**if** $R_1 > R_2$: D_1 is before and D_2 is after DBS;
  else:**else**: D_2 is before and D_1 is after DBS;
close the communication & return

may host many requests from different AIoT clients in corresponding sessions, as far as it can handle by its computing capability.

The detailed algorithms for the AIoT clients and the facial diagnosis server are listed in List I. In an AIoT server, the Pallier cryptosystem is set up to encrypt the query data for privacy protection. The encrypted data is then sent to the server side for medical diagnosis. The server will then carry out the computation in a layer-wise mode, and at each layer, will send the tentative outputs from each layer back to the client for the computation of activation or softmax, which needs both division and exponential operations. Once the computation at the server side reaches the last layer of deep neural networks, the final result will be sent back to the client and the communication session will be terminated.

In this framework, the server can maintain multiple sessions with different clients, as far as multi-threading is allowed on

Algorithm 2: Keyless Private Facial Diagnosis.

Inputs :

(1) Client lists with IDs and Passwords
(2) Pretrained weights w_{ij} and bias b_j
(3) From client: Query data $[\![D_k]\!]$ and $[\![1]\!]$

Procedure :

1: Setup DNNs with weights wij and bias bj;
2: wait for the client request:
3: verify user and setup the session;
4: wait for the client data $[\![D_k]\!]$ and $[\![1]\!]$:
5: loop over layers of the diagnosis DNN:
6: calculate $[\![y_j]\!]$ in layer-wise;
7: shuffle $[\![y_j]\!]$ over j randomly;
8: calculate $[\![z_j]\!]$ by querying the client (sigmoid);
9: end loop
10: calculate $[\![r_j]\!]$ by querying the client (softmax);
11: send the final results back to the client
12: close the session
13: return to step 2

the cloud server. It is worth noting that all keys (both public and private) are kept only on the client itself, and the computation at the server side is keyless and only needs an encrypted big integer $[\![1]\!]$.

B. Proposed AIoT Edge Service

As shown in Fig. 5, the proposed AIoT medical diagnosis framework is based on two-party communication in its computation. Though a server can host many clients, the communication session is based on a client with a communication channel to the server. Hence, there is a need to look into the data privacy issue of the two-party secure computation.

1) Privacy With Information Theoretical Security: An algorithm is defined as information-theoretically secure if its security is proved to match with the derived concept from information theory. The information-theoretical security in communication was termed by Shannon to prove that the one-time pad system achieves perfect security subject to the following two conditions [42]:

1) the key which randomizes the data should be random and should be used only once;
2) the key length should be at least as long as the length of the data.

If any algorithm randomizes its parameter and satisfies the above conditions, its parameters cannot be unmasked by an adversary even when the adversary has unlimited computing power. In this case, the system is guaranteed to have information theoretical security. If for example both the plain text and the random ciphertext have 1024 bits, the prior probability (probability for a particular ciphertext out of 2^{1024} possible ciphertexts) and posterior probability (probability of inferring/mapping a ciphertext in a random domain to a plaintext domain) are equal, and there is no advantage for an adversary to get higher posterior probability than prior probability.

In the following sections, we will analyze whether our algorithm in List I is vulnerable to any privacy leakage. Our algorithm is based on two party computation over the AIoT scheme. As defined by Goldreich [43], privacy for secure two-party computation will be achieved if a secure two-party protocol cannot reveal more information to a semi-honest party than the information that can be inferred by looking at that party's input and output. To verify whether the proposed AIoT computation satisfies the privacy definition, we will show the inputs and outputs to and from the client and server, respectively, in the algorithm in List I, and identify what is already known to the client and the server. Following this, if we can prove that nothing else can be inferred other than the known input and output with higher posterior probability than prior probability, the proposed algorithm in List I then satisfies with the privacy definition based on information theory.

The ultimate aim for the client is to keep the test image and the classification result away from the server while the server wants to keep the classification model parameters away from the client. In the communication, the client sends only the encrypted messages to the server with no public keys. From these inputs, the server knows only the size of the test image and the length of encrypted data. This is not a privacy leakage since the server knows the size of the images when training the classifier.

2) Privacy-Preserving Secure Computation At Edge: The overall framework needs its computation to be based on secure operations in both AIoT clients and the server. An honest-but-curious server/client follows the protocol and takes no actions beyond those of an honest server/client. In the proposed framework, let us assume the client knows a vector (data) $\mathbf{a}$ and sends its ciphertext $[\![\mathbf{a}]\!]$ to the server. The whole system will expect the ciphertext is unbreakable in both the server and any third party. Since the encrypted DNNs at the server side need neither private keys nor public keys, the security of the client data in the proposed AIoT-oriented keyless medical diagnosis system is therefore guaranteed, though asymmetric encryption can be breakable if public keys are available [39], [40].

The proposed two-party AIoT protocol in List I is information-theoretically secure i.e., the server cannot infer the plaintexts in the client's input vector $[\![\mathbf{a}]\!]$ and the client will only learn the final result but not the model parameters in the server.

To validate the security we consider both the client and server are honest-but-curious (HBC) i.e., they will follow the procedures but try to learn about each other's inputs, intermediate values and results. We will then demonstrate that the algorithm in List I is information-theoretically secure for the following two cases in 3) and 4).

3) Honest-But-Curious AIoT-oriented Server: The server computes the results in their encrypted form. Each layer performs a weighted summation, as shown in Eq.(8) and (10). The HBC client sends its encrypted data to the server, and the server computes the weighted sum outputs and shuffle them via one time pad, and send them back to the client for the computation. Because the inputs and the outputs are shuffled each time using different one-time pads (step 7 in algorithm 2, List I), the client cannot accumulate the knowledge to solve w_{ij} and b_j in Eq.(8). Hence, there is no privacy leak on model parameters such as weights and bias values in layers, and the communication from the server to the client is perfectly information theoretical secure in term of the server's private model.

4) Honest-But-Curious AIoT-oriented Server: The main purpose in the proposed framework is to protect the data privacy of the individual client from the public medical diagnosis server. In List I, a client encrypts its data and sends the data to the server, and the server carries out its computation on encrypted data only, and return the encrypted result back to the client, which implies that only the client can know the final results via decryption.

However, as has been suspected [36], [37], asymmetric encryption itself may not be information theoretical secure, since the factorization of a large prime number can be solved via some algorithms [36] in limited time, if the public keys can be known. However, in our proposed algorithms in List I, neither private keys nor public keys are shared with the server. The curious server cannot infer the keys simply from the ciphertext.

It is worth noting that in the proposed scheme, the encryption of 1 needs to be sent to the server. Considering $t = 1$, we have

$$c1 = [\![1|r]\!] = \mathrm{mod}\left(gr^n, n^2\right), \text{and } c \in Z^*_{n^2} \tag{12}$$

and,

$$1 = \langle c1 \rangle = \mathrm{mod}\left(\frac{\mathrm{mod}\left(c^\lambda, n^2\right) - 1}{n}\mu, n\right) \tag{13}$$

In the above equations, g, r, n, c and λ are all unknown to the server side, and these parameters are changed every time based on one time pad strategy. Hence, the server cannot accumulate more knowledge about the encryption parameters from the next ciphertext, and the private data from the client will be information theoretical secure to the server side.

C. Information Theoretical Security in Our Framework

It is noted that though the computation is split between the AIoT edge side and the cloud server side, the computation is information secure and neither side can infer from the data for more than necessary information. In the server side, the model weights and bias will not be learned by an edge user because they are randomly shuffled every time in the step 7 in the algorithm 2 in List I. Meanwhile, both public and private keys are unknown to the server side, and therefore a user's own data will not be exposed to the service provider via some cracking algorithms such as Shor's algorithm [36]. Therefore, information theoretical security is guaranteed in both edge client and cloud server sides by our novel implementation.

V. Experiments

A. PD DBS Dataset From Youtube

In our experiment, we use a video dataset consisting of 52 PD patients collected from Youtube online resources. Two video shots were taken per patient before and after DBS treatment. From videos, we extract 2345 facial images for our tests, as shown in Fig. 6. The facial images were cropped from video shots and resized to 32×32 pixels. The dataset is then split into

Fig. 6. PD DBS facial dataset and encrypted faces.

two subsets – training dataset and test dataset, each having 26 PD patients.

In our experiments, it is assumed that the training dataset is owned by the server to train the deep neural networks for medical diagnosis, and the test dataset is owned as private data by AIoT clients. The experiments were set up as a cross-subject facial diagnosis test, while training faces and test faces are from different subjects/patients. Such cross-subject issues are often considered more challenging than the same subject tests (such as recognize a face of a person already in the training dataset).

Our experiments are set up as below. Given two images of a patient, one from before the DBS treatment and one from after the treatment, we want to know:

1) Can facial features be used to clearly discriminate which one is before or after DBS treatment?
2) Can the proposed lightweight PHE-based solution work properly as an implementation of private deep learning?
3) Can our PHE-based solution achieve an accuracy similar to its original non-privacy-preserving peer?

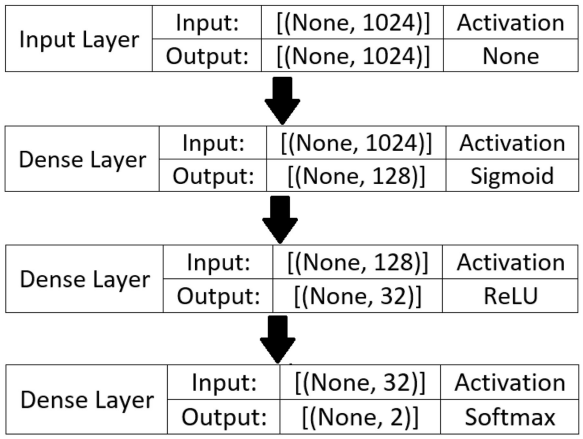
To answer the above questions, our experiments are detailed in the following sections.

B. Facial Diagnosis Using Deep Neural Networks

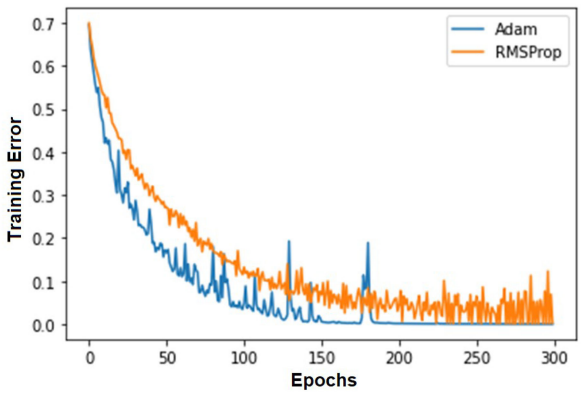
Although facial expression is known to be associated with the degree of Parkinson's, it is yet not used on the evaluation of DBS treatment. To achieve this purpose, we aim to exploit deep neural networks to carry out the facial diagnosis on the patients.

In our experiments, our targets is to demonstrate the proposed PHE based lightweight implementation of deep neural networks over encrypted data. We choose Deep Autoencoder as our classifier because it is the first reported method that enlightened the research on deep learning [44]. Here, we only need the encoder part, as shown in Fig. 7a, a four layer deep neural network architecture with two hidden dense layers. It takes all dimensions of the data as its inputs, and then reduces the number of neurons via the propagation from layer to layer, from 1024, 128 to 32.

In our implementation, the input layer has $32 \times 32 = 1024$ neurons. The 1st hidden layer has 128 neurons with sigmoid activation, and the 2nd hidden layer has 32 neurons with ReLU activation. The output layer with softmax activation has two neurons standing for two classes: before DBS treatment (with apparent PD symptoms) and after DBS treatment (with little PD symptoms).



(a) The structure of the deep encoder as a classifier



(b) Training the classifier in the server side. Two training methods, Adam and RMSProp were used.

Fig. 7. Train the deep encoder classifies on the server side.

TABLE II
EVALUATION ON THE CROSS-SUBJECT DATASET

Method	Precision	Recall	Acc	F1
Adam	94.88%	94.28%	94.71%	94.54%
RMSProp	96.20%	95.00%	95.22%	95.10%

We used the training dataset (facial images of 26 patients) trained the four layer encoder, and obtained the model parameters. Fig. 7b) shows the convergence of loss rates in the training process. Here, two training methods were applied, Adam and RMSProp. We can see the model trained by RMSProp achieved better accuracy.

Table II shows the valuation on two trained models in term of accuracy, recall, precision and F1 score based on the output likelihoods on two classes. We can see the RMSProp based model achieved a bit better results consistently on all measures. Hence, we use the RMSProp model as our facial diagnosis service model.

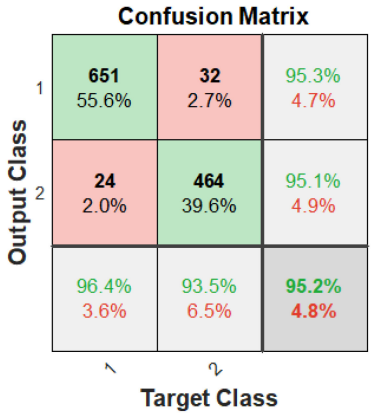


Fig. 8. Confusion matrix of the facial diagnosis test.

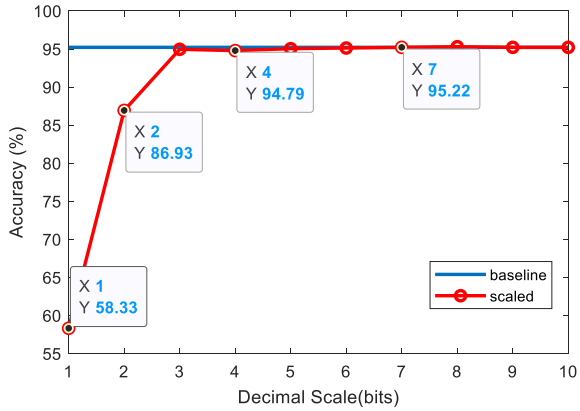


Fig. 9. Test accuracy over the decimal precision of the encrypted DNN model parameters.

TABLE III
PREDIAGNOSIS USING FACE VS USING MRI

Method	Clinical Cases	Accuracy
MRI-based Prediagnosis [45]	13 Patients	84.62%
Our Facial Prediagnosis	52 Patients	95.22%

Fig. 8 shows the confusion matrix of the test results. We can clearly see that the model achieved a nice accuracy over 95%, implying that there are sufficiently explicit facial features to discriminate a PD patient form a recovered patient.

It is worth to note that the diagnosis is based on a single facial photo instead of long shot videos, and the test subjects are all new to the trained model. From the test results, we can clearly see the trained model can explicitly discriminate the faces of patients before and after DBS treatment, suggesting its potential as an automated medical diagnosis tool for evaluating the severity of PD patients.

In Table III, we compared the facial prediagnosis against the MRI-based prediagnosis in clinical trials. MRI-based preclinical assessment achieved its accuracy around 85%, as reported by an Oxford team from their clinical trial with 13 patients. In comparison, our facial prediagnosis on 52 patients achieved an initial accuracy around 95.22%. It is also worth to highlight that unlike the expensive EEG based diagnosis, facial prediagnosis could be low-cost, non-interrupting, and available 24/7 remotely with little needs of staff intervention, demonstrating a great potential as a new prediagnosis tool on PD for medical caring services.

C. Encrypted Facial Diagnosis Over AIoT Edge

Following the test in the above section, we implemented the encrypted counterpart of the above facial diagnosis model and compare the test results on the encrypted test dataset. Here, a concern issue is about the number of decimal digits that may scale down the model parameters (weights, bias, etc). The encrypted data from a client was fed to the encrypted DNN model on the server side, and we want to examine if the algorithms in List I can achieve similar accuracy as the original non-privacy-preserving model even with a reduced or limited number of decimal digits.

TABLE IV
COMPUTATIONAL TIME VERSUS THE BIT LENGTH ON SERVER AND CLIENT, MEASURED IN SECONDS AVERAGED PER TEST IMAGE IN OUR EXPERIMENT

Bits	256	512	768	1024
Server (s)	42	64	101	146
Clients (s)	1	2	5	9
Total (s)	43	66	106	155

Fig. 9 shows the comparison of the results of the encrypted implementation with different decimal precisions. The decimal precision varies from 1 bit to 10 bit, and we valuated the classification accuracy on the encrypted data. We can see that when decimal bits were reduced to 1 bit (2^{-1} or 0.5), the accuracy was only 58.33%. When the decimal bits were increased to 7 bits, the encryption-based model achieved the same accuracy (95.22%) as its non-privacy preserving original model. Compared with the length of big integer, 7 bits for decimal digits could be a small cost for the overall encryption scheme.

Table IV also gives the experimental results on the computational time in the client and the server, respectively, over various bit lengths of the big integer. Here both client and server were running on a GPU-powered laptop with 3.6GHz CPU. The results show that in the same session, most computational work load (∼95%) was assigned to the server side, which is a benefit for AIoT end users offered by the service provider. Typically, the computational time can be linked to the computational complexity, as analyzed below.

D. Computational Complexity

The computational complexity of the algorithm in List I can be estimated as the costs of two types of big integer operations: multiplication operations and modulo exponentiation as C_m and C_e, respectively. Table V list out the estimated complexity of the proposed schemes for both the server (S) and client (C) with regards to the number of neurons per layer ($m_0, m_1, etc.$) and the number of synaptic inputs to each neuron (namely the number

TABLE V
ESTIMATED COMPUTATIONAL COMPLEXITY

Layers	Server	Client
Input	0	$m_0(2C_e+C_m)$
Layer 1	$m_1m_0(C_e+C_m)$	$3m_1(C_e+C_m)$
Layer 2	$m_2m_1(C_e+C_m)$	$3m_2(C_e+C_m)$
Layer 3	$m_3m_2(C_e+C_m)$	$3m_3(C_e+C_m)$
Total	$(m_3m_2+m_2m_{1+}m_1m_0)$ $\times(C_e+C_m)$	$(2m_0+3m_1+3m_2+3m_3)C_e$ $+(m_0+3m_1+3m_2+3m_3)C_m$

TABLE VI
COMMUNICATION COMPLEXITY

Layers	S2C	C2S
Input layer	0	m_0C_{Big}
Layer 1	m_1C_{Big}	m_1C_{Big}
Layer 2	m_2C_{Big}	m_2C_{Big}
Layer 3	m_3C_{Big}	0
Total	$(m_1+m_2+m_3)\times C_{Big}$	$(m_0+m_1+m_2)\times C_{Big}$

of neurons in the previous layer, in the architecture illustrated in Fig. 4).

In our implementation, the input layer has 32×32 neurons, layer 1 has 128 neurons, layer 2 has 32 neurons and the final layer has 2 neurons. Hence, the total computational costs can be estimated as:

Server side: $(1024\times128+128\times32+32\times2)\rightarrow135232\times(C_e+C_m)$

Client side: $2534\times C_e+1510\times C_m$

We can see most computational workload is assigned to the server side. Assuming $C_e \approx C_m$, the ratio of the workload between the server and a client is 135232/4044 ≈ 36.1, which implies the server copes with 97% of the total computation. This theoretical analysis matches well with the experimental results (∼95%) in Table V. Since the cloud-based server has much better computation resources, such a client-server split is reasonable for an AIoT edge-oriented framework.

Besides the computation on the cipher texts, the computational cost on encryption is a constant that is proportional to the number of pixels per facial photo. In this experiment, each photo has $32\times32 = 1024$ pixels. Assuming the encryption on each pixel has an encryption cost C_E, the extra computation cost per facial photo will then be $1024C_E$.

E. Communication Complexity

We can measure the total communication complexity in terms of data being communicated between the server and client. In our algorithm, the transferred data between client and server are all in the form of big integer, such as 1024-bit format, as detailed in the secure two-party algorithm proposed in List I. The estimated communication load is summarized in Table VI based on a layer-wise estimation in term of the communication costs of a single 1024-bit big integer, C_{Big}.

Similarly, since the input layer has 32×32 neurons, layer 1 has 128 neurons, layer 2 has 32 neurons and the final layer has 2 neurons, the total communication costs can be estimated as:

Server to client: $162\times C_{Big}$

Client to server: $1184\times C_{Big}$

In total, the communication bandwidth needs to cope with $1346\times C_{Big} = 1346\times1024$bits $= 1.378$Mbits. If we process video streams at 25 frames per seconds, the highest bandwidth needs to be around 35 Mbps. Currently 5G-based AIoT can easily achieve 100+ Mbps. Hence, the communication complexity in our proposed AIoT framework is achievable even in the case of considering real-time video streaming, although our facial diagnosis carries out on single image based classification.

VI. CONCLUSION

In conclusion, we have demonstrated a novel AIoT-oriented medical diagnosis framework using deep learning and PHE that can achieve Shannon's information theoretical security. In our proposed scheme, the encrypted DNNs at the server side were implemented without the needs for encryption keys, guaranteeing the client data has information theoretical security; the intermediate results from the server to a client were shuffled randomly, making the model unknown to the client, too. Hence, the information theoretical security at both server and client ends is guaranteed via our proposed framework, showing a promising merit toward the privacy protection on exploiting EHR/EMR data for wide medical services.

It is also worth noting that, with the 95.22% accuracy of our facial prediagnosis model, we verified that facial prediagnosis could be a valuable medical tool with a potential to evaluate the severity of PD patients. Consequently, we offered a novel low-cost method for the preclinical assessment on PD with an initial proof-of-concept test showing the underlying links between facial features and PD symptoms. One of our future tasks is to explicitly expand our deep facial prediagnosis to an explainable model, to help identify which part of facial features are linked to the severity of PDs.

Besides, we reported our facial prediagnosis model with a clinical trial on 52 PD patients before and after DBS treatment, which could also be valuable and interesting for many medical researchers, doctors, or clinical consultants. In the future work, a more clear evaluation on how facial features can be linked to evaluate the improvement of PD treatments can be further studied, aiming to bring Explainable AI and Fair AI into this privacy-sensitive topic [46].

REFERENCES

[1] F. Cheung, "TCM: Made in China," *Nature*, vol. 480, no. 7378, pp. 82–83, Dec. 2011.
[2] X. Li, D. Yang, Y. Wang, W. Zhang, F. Li, and W. Zhang, "Face parsing for traditional Chinese medicine inspection via a hybrid neural network," *IEEE Access*, vol. 18, pp. 93069–93082, 2020.
[3] Y. Gurovich *et al.*, "Identifying facial phenotypes of genetic disorders using deep learning," *Nature Med.*, vol. 25, pp. 60–64, 2019.
[4] S. Richmond *et al.*, "Facial genetics: A brief overview," *Front. Genet.*, Oct. 2018.
[5] D. J. M. Crouch *et al.*, "Genetics of the human face: Identification of large-effect single gene variants," *PNAS*, vol. 115, pp. E676–E685, 2018.
[6] C. M. Delude, "Deep phenotyping: The details of disease," *Nature*, vol. 527, pp. S14–S15, 2015.
[7] G. Storey, R. Jiang, R. S. Keogh, A. Bouridane, and C.-T. Li, "3DPalsyNet: A facial palsy grading and motion recognition framework using fully 3D

convolutional neural networks," *IEEE Access*, vol. 7, pp. 121655–121664, Aug. 2019.
[8] G. Storey, R. Jiang, and A. Bouridane, "Role for 2D image generated 3D face models in the rehabilitation of facial palsy," *IET Healthcare Technol. Lett.*, vol. 4, no. 4, pp. 145–148, 2017.
[9] E. R. Dorsey *et al.*, "Deep phenotyping of Parkinson's disease," *J. Parkinsons Dis.*, vol. 10, pp. 855–873, Jan. 2020.
[10] R. Krüger *et al.*, "Classification of advanced stages of Parkinson's disease: Translation into stratified treatments," *J. Neural Transmiss. (Vienna)*, vol. 124, pp. 1015–1027, 2017.
[11] S. Argaud *et al.*, "Facial emotion recognition in Parkinson's disease: A review and new hypotheses," *Movement Disord.*, vol. 33, pp. 554–567, 2018. doi: 10.1002/mds.27305.
[12] D. Bowers *et al.*, "Startling facts about emotion in Parkinson's disease: Blunted reactivity to aversive stimuli," *Brain*, vol. 129, pp. 3356–3365, Dec. 2006.
[13] C. Klein and A. Westenberger, "Genetics of Parkinson's disease," *Cold Spring Harb Perspect Med.*, vol. 2, no. 1, 2012, Art. no. a008888.
[14] D. Rial *et al.*, "Behavioral phenotyping of Parkin-deficient mice: Looking for early preclinical features of Parkinson's disease," *PLoS One*, vol. 9, 2014, Art. no. e114216.
[15] X. Liu, R. Lu, J. Ma, L. Chen, and B. Qin, "Privacy-preserving patient-centric clinical decision support system on naïve Bayesian classification," *IEEE J. Biomed. Health Informat.*, vol. 20, no. 2, pp. 655–668, Mar. 2016, doi: 10.1109/JBHI.2015.2407157.
[16] X. Yang, R. Lu, J. Shao, X. Tang, and H. Yang, "An efficient and privacy-preserving disease risk prediction scheme for e-healthcare," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 3284–3297, Apr. 2019, doi: 10.1109/JIOT.2018.2882224.
[17] X. Liu, R. H. Deng, K. R. Choo, and Y. Yang, "Privacy-preserving outsourced support vector machine design for secure drug discovery," *IEEE Trans. Cloud Comput.*, vol. 8, no. 2, pp. 610–622, Apr.–Jun. 2020, doi: 10.1109/TCC.2018.2799219.
[18] J. Feng, L. T. Yang, Q. Zhu, and K. R. Choo, "Privacy-preserving tensor decomposition over encrypted data in a federated cloud environment," *IEEE Trans. Dependable Secure Comput.*, vol. 17, no. 4, pp. 857–868, Jul./Aug. 2020, doi: 10.1109/TDSC.2018.2881452.
[19] H. Zhu, X. Liu, R. Lu, and H. Li, "Efficient and privacy-preserving online medical prediagnosis framework using nonlinear SVM," *IEEE J. Biomed. Health Informat.*, vol. 21, no. 3, pp. 838–850, May 2017, doi: 10.1109/JBHI.2016.2548248.
[20] X. Sun, P. Zhang, J. K. Liu, J. Yu, and W. Xie, "Private machine learning classification based on fully homomorphic encryption," *IEEE Trans. Emerg. Topics Comput.*, vol. 8, no. 2, pp. 352–364, Apr.–Jun. 2020.
[21] Y. Rahulamathavan, S. Veluru, R. Phan, J. Chambers, and M. Rajarajan, "Privacy-preserving clinical decision support system using Gaussian kernel based classification," *IEEE J. Biomed. Health Informat.*, vol. 18, no. 1, pp. 56–66, Jan. 2014.
[22] Z. Erkin, M. Franz, J. Guajardo, S. Katzenbeisser, I. Lagendijk, and T. Toft, "Privacy-preserving face recognition," in *Proc. 9th Int. Symp. Privacy Enhancing Technol.*, 2009, pp. 235–253.
[23] Y. Rahulamathavan, R. Phan, J. Chambers, and D. Parish, "Facial expression recognition in the encrypted domain based on local fisher discriminant analysis," *IEEE Trans. Affect. Comput.*, vol. 4, no. 1, pp. 83–92, Jan.–Mar. 2012.
[24] Y. Rahulamathavan and M. Rajarajan, "Efficient privacy-preserving facial expression classification," *IEEE Trans. Dependable Secure Comput.*, vol. 14, no. 3, pp. 326–338, May 2017.
[25] R. Jiang, A. Bouridane, D. Crookes, M. E. Celebi, and H.-L. Wei, "Privacy-protected facial biometric verification using fuzzy forest learning," *IEEE Trans. Fuzzy Syst.*, vol. 24, no. 4, pp. 779–790, Aug. 2016.
[26] A. Alharthi, Q. Ni, and R. Jiang, "A privacy-preservation framework based on biometrics blockchain (BBC) to prevent attacks in VANET," *IEEE Access*, vol. 9, pp. 87299–87309, 2021.
[27] F. A. Khan, A. Bouridane, S. Boussakta, R. Jiang, and S. Almaadeed, "Secure facial recognition in the encrypted domain using a local ternary pattern approach," *J. Inf. Secur. Appl.*, vol. 59, 2021, Art. no. 102810.
[28] H. Lipmaa, S. Laur, and T. Mielikainen, "Cryptographically private support vector machines," in *Proc. 12th ACM SIGKDD Int. Conf. Knowl. Discov. Data Mining*, Aug. 2006, pp. 618–624.
[29] M. Barni *et al.*, "Privacy-preserving fingercode authentication," in *Proc. 12th ACM Workshop Multimedia Secur.*, 2010, pp. 231–240.
[30] W. Du and Z. Zhan, "Building decision tree classifier on private data," in *Proc. IEEE Int. Conf. Privacy Secur. Data Mining*, vol. 14, pp. 1–8, 2002.
[31] E. Hesamifard, H. Takabi, and M. Ghasemi, "CryptoDL: Deep neural networks over encrypted data," 2017. [Online]. Available: https://arxiv.org/abs/1711.05189
[32] N. Dowlin *et al.*, "CryptoNets: Applying neural networks to encrypted data with high throughput and accuracy," in *Proc. 33rd Int. Conf. Mach. Learn.*, 2016, vol. 48, pp. 201–210.
[33] Q. Zhang, C. Wang, H. Wu, C. Xin, and T. V. Phuong, "GELU-Net: A globally encrypted, locally unencrypted deep neural network for privacy-preserved learning," in *Proc. Twenty-7th Int. Joint Conf. Artif. Intell.*, 2018, pp. 3933–3939.
[34] K. Nandakumar, N. Ratha, S. Pankanti, and S. Halevi, "Towards deep neural network training on encrypted data," in *Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. Workshops*, 2019, pp. 1–9.
[35] T. Ryffel1, E. Dufour-Sans, R. Gay, F. Bach, and D. Pointcheval, "Partially encrypted machine learning using functional encryption," in *Proc. 33rd Conf. Neural Inf. Process. Syst.*, Vancouver, Canada, 2019, pp. 1–21.
[36] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in *Proc. 35th Annu. Symp. Foundations Comput. Sci.*, 1994, pp. 124–134.
[37] M. Amico, Z. H. Saleem, and M. Kumph, "An experimental study of shor's factoring algorithm on IBM Q," *Phys. Rev. A*, vol. 100, no. 1, 2019, Art. no. 012305.
[38] P. Easom-Mccaldin, A. Bouridane, A. Belatreche, and R. Jiang, "On depth, robustness and performance using the data re-uploading single-qubit classifier," *IEEE Access*, vol. 9, pp. 65127–65139, 2021.
[39] C. Zhao *et al.*, "Secure multi-party computation: Theory, practice and applications," *Informat. Sci.*, vol. 476, pp. 357–372, 2019.
[40] D. Evans, V. Kolesnikov, and M. Rosulek, *A Pragmatic Introduction to Secure Multi-Party Computation*. Norwell, MA, USA: NOW, 2018.
[41] K. A. Jagadeesh, D. J. Wu, J. A. Birgmeier, D. Boneh, and G. Bejerano, "Deriving genomic diagnoses without revealing patient genomes," *Science*, vol. 357, pp. 692–695, 2017.
[42] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, 1949.
[43] O. Goldreich, "Secure multiparty computation," Sep. 1998. [Online]. Available: http://www.wisdom.wei zmann.ac.il/oded/pp.html
[44] Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," *Nature*, vol. 521, no. 7553, pp. 436–444, 2015.
[45] K. Szewczyk-Krolikowski *et al.*, "Functional connectivity in the basal ganglia network differentiates PD patients from controls," *Neurology*, vol. 83, no. 3, pp. 208–214, Jul. 2014.
[46] P. Angelov, E. Almeida Soares, R. Jiang, N. Arnold, and P. Atkinson, "Explainable artificial intelligence: An analytical review," in *WIREs Data Mining and Knowledge Discovery*. 2021, Hoboken, NJ, USA: Wiley.