Security Analysis of “PSLP: Privacy-Preserving Single-Layer Perceptron Learning for e-Healthcare”

Jingjing Wang[1], Xiaoyu Zhang[1], Jingjing Guo[1], and Jianfeng Wang[1]

[1] State Key Laboratory of Integrated Service Networks (ISN),
Xidian University, Xi’an, P.R. China
jingjw123@163.com,moliyanyan@163.com,jiaozuoguojing@163.com
jfwang@xidian.edu.cn

Abstract. With the synchronous development of both cloud computing and machine learning techniques, the clients are preferring to resort to the cloud server with substantial resources to train learning model. However, in this outsourcing paradigm it is of vital significance to address the privacy concern of client’s data. Many researchers have been focusing on preserving the privacy of client’s data in learning model. Recently, Wang et al. presented a privacy-preserving single-layer perceptron learning for e-healthcare scheme with using paillier cryptosystem and claimed that their scheme can protect the privacy of user’s medical information. By analysing the process of iteration and the communication between the cloud and the user, we present that the honest-but-curious cloud can obtain the private medical information. Besides, the leakage of medical cases will lead to the exposure of the specific single-layer perceptron model of e-healthcare, which has gigantic commercial value.

Keywords: Outsourcing computation, Single-layer perceptron neural network, Privacy preservation, Paillier cryptosystem

1 Introduction

With the rapid development of cloud computing, cloud storage and the data collection capacity, an era of big data is now under way [1]. In the era of big data, it is common to extract useful information from large databases by using the techniques of data mining and machine learning [2]. Among these techniques, neural network model with strong ability to learn the feature of big data is often used to predict outputs efficiently, which has drawn more attention in recent years. Considering a huge amount of data and the complexity of the construction of neural network model, users are inclined to outsource their data and computation to the cloud server.

However, the openness and heterogeneity of the network inevitably brings the security problems to data stored in the cloud server. Therefore, the outsourcing paradigm will bring a potential threat to user’s privacy information. In order to address the above privacy preserving problem, several related works have been proposed [3][4][5].

Recently, Wang et al. [3] have proposed an efficient privacy-preserving single-layer perceptron learning (PSLP) scheme by using paillier cryptosystem. In the PSLP system, hospital outsources the ciphertext of medical cases and heavy calculation tasks to the cloud server, which is honest-but-curious. However, the cloud server can obtain the sensitive medical data and the final optimal weight vector in the training process. In the following, we will review their PSLP scheme and point out a security weakness based on that one linear equation with one unknown number $\vec{w}_j = \vec{w}_j + \eta y_i \vec{x}_{i,j}$ (for $1 \leq j \leq n$) can be solved.

2 Review of the PSLP Scheme

In this section, we will overview the PSLP scheme, which is composed of two stages: system setting and privacy-preserving single-layer perceptron learning.

2.1 Notations

In order to facilitate reading, we first present some notations.

- m: the number of medical case.
- n: the feature number of a piece of medical case.
- $\vec{x}_i$: a piece of medical case, $\vec{x}_i = (x_{i,1}, \cdots, x_{i,n})$ ($i \in \{1, \cdots, m\}$).
- $e\vec{x}_i$: the ciphertext of a piece of medical case, $e\vec{x}_i = (ex_{i,1}, \cdots, ex_{i,n})$ ($i \in \{1, \cdots, m\}$).
- y_i: the label or desired output of a piece of medical case, $i \in \{1, \cdots, m\}$, $y_i = -1$ denotes class C_1 and $y_i = 1$ denotes class C_2.
- $\vec{w}$: a weight vector, $\vec{w} = (w_1, \cdots, w_n)$, w_j ($j \in \{1, \cdots, n\}$) is corresponding to $x_{i,j}$ (for $1 \leq i \leq m$). In the mean while, $\vec{w}^{(t)}$ means the weight vector which is updated by $t-1$ times, t is a positive integer number.
- $e\vec{w}$: the ciphertext of weight vector $\vec{w}$, $e\vec{w} = (ew_1, \cdots, ew_n)$. In the mean while, $e\vec{w}^{(t)}$ means the ciphertext of weight vector which is updated by $t-1$ times, t is a positive integer number.
- $sign(z)$: a sign function, if $z \geq 0$, output 1; otherwise output -1.
- N: the product of two large prime numbers in paillier cryptosystem, it is public.
- η: learning rate of the single-layer perceptron learning model.

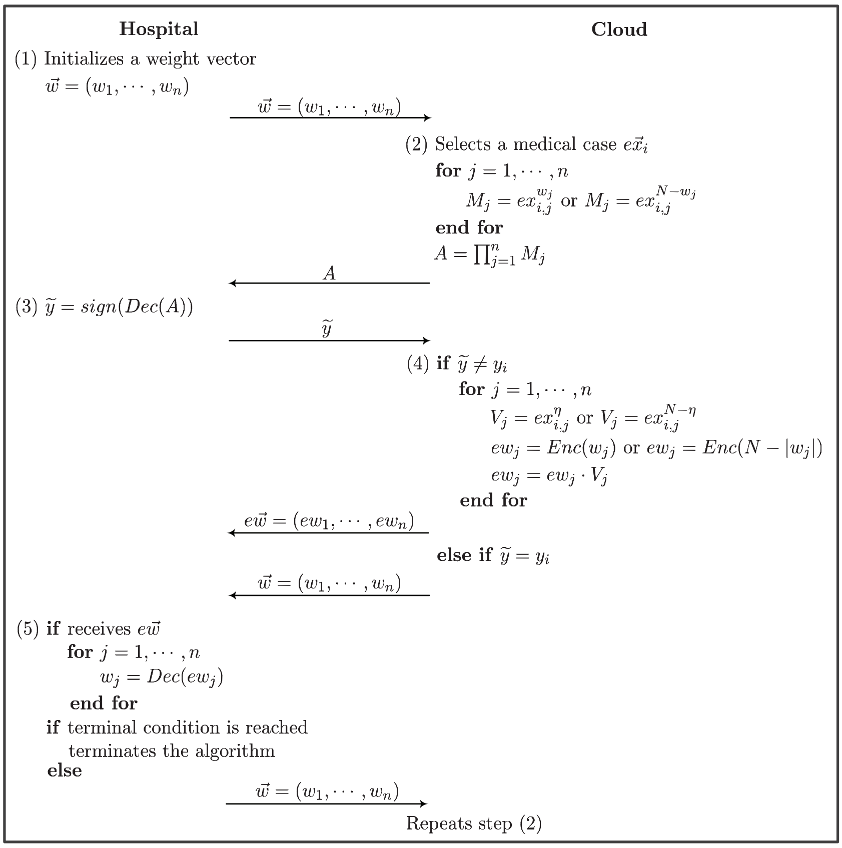
2.2 PSLP Scheme

We briefly review the PSLP scheme below.

- **System setting.** The hospital runs the paillier cryptosystem's key generation algorithm to obtain the public key PK, and the private key SK according to the security parameter k. And then, the hospital runs the paillier encryption algorithm $Enc(\cdot)$ to encrypt the medical cases $x = \{\vec{x}_1, \cdots, \vec{x}_m\}$

with the public key PK, and obtains the corresponding ciphertexts $ex = \{e\vec{x}_1, \cdots, e\vec{x}_m\}$. Afterwards, the hospital sends the ciphertexts ex and the desired outputs $\{y_1, \cdots, y_m\}$ $(y_i \in \{-1, 1\})$ to the cloud server.

- **Privacy-preserving single-layer perceptron learning.** The main steps of the PSLP scheme are described in Fig. 1.



```
Hospital                                          Cloud
(1) Initializes a weight vector
    $\vec{w} = (w_1, \cdots, w_n)$
                 $\vec{w} = (w_1, \cdots, w_n)$ →
                                          (2) Selects a medical case $e\vec{x}_i$
                                              for $j = 1, \cdots, n$
                                                  $M_j = ex_{i,j}^{w_j}$ or $M_j = ex_{i,j}^{N-w_j}$
                                              end for
                                              $A = \prod_{j=1}^{n} M_j$
                 ← $A$
(3) $\widetilde{y} = sign(Dec(A))$
                 $\widetilde{y}$ →
                                          (4) if $\widetilde{y} \neq y_i$
                                                  for $j = 1, \cdots, n$
                                                      $V_j = ex_{i,j}^{\eta}$ or $V_j = ex_{i,j}^{N-\eta}$
                                                      $ew_j = Enc(w_j)$ or $ew_j = Enc(N - |w_j|)$
                                                      $ew_j = ew_j \cdot V_j$
                                                  end for
                 ← $e\vec{w} = (ew_1, \cdots, ew_n)$
                                              else if $\widetilde{y} = y_i$
                 ← $\vec{w} = (w_1, \cdots, w_n)$
(5) if receives $e\vec{w}$
        for $j = 1, \cdots, n$
            $w_j = Dec(ew_j)$
        end for
    if terminal condition is reached
        terminates the algorithm
    else
                 $\vec{w} = (w_1, \cdots, w_n)$ →
                                          Repeats step (2)
```

Fig. 1. The Process of PSLP Scheme

- **Step 1:** The hospital initializes a weight vector $\vec{w} = (w_1, \cdots, w_n)$, and sends it to the cloud server.
- **Step 2:** The cloud server obtains the weight vector $\vec{w} = (w_1, \cdots, w_n)$, and then selects a piece of ciphertext of medical information $e\vec{x}_i = (ex_{i,1}, \cdots, ex_{i,n})$ $(i \in \{1, \cdots, m\})$, then calculates $M_j = ex_{i,j}^{w_j}$ $(w_j \geq 0)$ or $M_j = ex_{i,j}^{N-|w_j|}$ $(w_j < 0)$ (for $1 \leq j \leq n$) and $A = \prod_{j=1}^{n} M_j$. The cloud server returns A to the hospital.
- **Step 3:** The hospital obtains the ciphertext A and decrypts it with paillier decryption algorithm $Dec(\cdot)$, and then calculates the value of the function $sign(\cdot)$ where we denote $\widetilde{y} = sign(Dec(A))$. The value of $\widetilde{y}$ is sent to the cloud server.

- **Step 4:** After receiving the $\widetilde{y}$, the cloud server compares the $\widetilde{y}$ with the desired output y_i. If $\widetilde{y} \neq y_i$, calculates $V_j = ex_{i,j}^{\eta}(y_i = 1)$ or $V_j = ex_{i,j}^{N-\eta}(y_i = -1)$. In the meanwhile, the cloud server encrypts the weight vector $\vec{w}$ by using paillier encryption algorithm $Enc(\cdot)$, $ew_j = Enc(w_j)$ $(w_j \geq 0)$ or $ew_j = Enc(N - |w_j|)$ $(w_j < 0)$ (for $1 \leq j \leq n$). And then, the cloud server calculates $ew_j = ew_j \cdot V_j$ (for $1 \leq j \leq n$) to update weight vector $\vec{w}$. Ultimately, the cloud server sends back the ciphertext of updated weight vector $e\vec{w}$ to the hospital. If $\widetilde{y} = y_i$, the plaintext of weight vector $\vec{w}$ will be returned to the hospital. Note that the weight vector is encrypted only once when it is updated in the first time.
- **Step 5:** If the hospital receives the ciphertext of weight vector $e\vec{w}$, it obtains $\vec{w}$ by using the paillier decryption algorithm $w_j = Dec(ew_j)$ (for $1 \leq j \leq n$), and sends the decrypted plaintext $\vec{w}$ to the cloud server, then the cloud server continues to run from step 2. The hospital will terminate the training process if one or more of the following conditions are satisfied. The first condition is that the number of iterations is larger than a preset threshold, and the second condition is that the weight vector hospital received is plaintext for every medical case.

3 Security Analysis of the PSLP Scheme

Because the medical information $x = \{\vec{x}_1, \cdots, \vec{x}_m\}$ has tremendous commercial value, the honest-but-curious cloud server may want to obtain the privacy medical information. In this section, we will show a honest-but-curious cloud server is able to obtain the private medical information in the PSLP scheme.

Let $\mathscr{A}$ be an honest-but-curious cloud server, it is able to obtain the private medical information. That is, in an iteration process, if $\mathscr{A}$ updates the weight vector $\vec{w}$, it would obtain the plaintext of updated weight vector $\vec{w}$ returned by the hospital as described in step 5 of section 2. Then, $\mathscr{A}$ possesses the plaintext of weight vector $\vec{w}$ before updating, the plaintext of updated weight vector $\vec{w}$, the learning rate η and the desired output y_i. Trivially, $\mathscr{A}$ can obtain the values of medical case $\vec{x}_i = (x_{i,1}, \cdots, x_{i,n})$ according to the linear equation with one unknown number $\vec{w}_j = \vec{w}_j + \eta y_i \vec{x}_{i,j}$ (for $1 \leq j \leq n$). Therefore, the cloud server can obtain the private medical information $\vec{x}_i$ by solving these equations. Furthermore, the more times the algorithm iterates, the more medical cases will be leaked.

Besides, if the medical cases are disclosed, it would be easier for $\mathscr{A}$ to know the practical meaning of each feature value corresponding weight vector $\vec{w}$. However, in the PSLP scheme, $\mathscr{A}$ can also obtain the final optimal weight vector $\vec{w} = (w_1, \cdots, w_n)$, when the terminal condition is the second one as described in step 5 of section 2. Therefore, the leakage of medical cases will lead to the exposure of the specific single-layer perceptron model for e-healthcare. However, the model also has gigantic commercial value.

In the following, we analyze the reason for security weakness of the PSLP scheme. The main cause is that the cloud server must obtain the plaintext of the weight vector $\vec{w}$ in order to calculate the $\vec{w} \cdot \vec{x}_i (i \in \{1, \cdots, m\})$ by using paillier cryptosystem. Trivially, if the cloud server obtains the plaintext of weight vector $\vec{w}$ before updating and the updated weight vector $\vec{w}$, it would be easy to obtain the medical case $\vec{x}_i$ by solving this linear equation with one unknown vector $\vec{w} = \vec{w} + \eta y_i \vec{x}_i$. Besides, the plaintext of medical cases greatly increase the probability of guessing the meaning of each feature value correctly for the cloud server.

Here we describe above steps by a concrete example as below. Suppose $w_j^{(1)} \geq 0$ (for $1 \leq j \leq n$), $y_1 = 1$, $\widetilde{y} = -1$. The main steps of this example are concluded in Fig. 2.

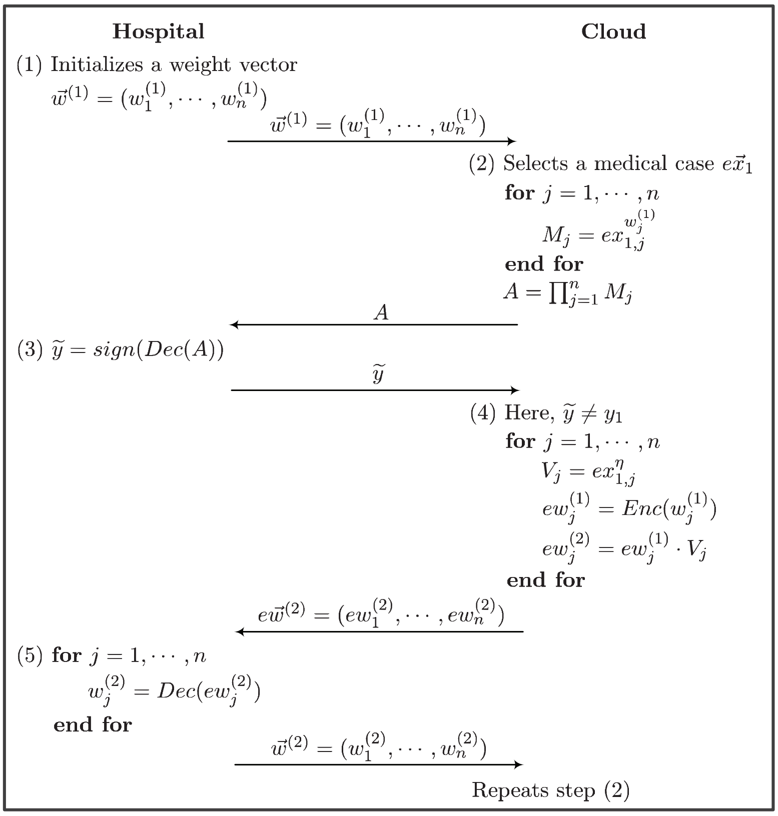

Hospital
Cloud
(1) Initializes a weight vector
$\vec{w}^{(1)} = (w_1^{(1)}, \cdots, w_n^{(1)})$
$\vec{w}^{(1)} = (w_1^{(1)}, \cdots, w_n^{(1)})$
(2) Selects a medical case $e\vec{x}_1$
for $j = 1, \cdots, n$
$M_j = ex_{1,j}^{w_j^{(1)}}$
end for
$A = \prod_{j=1}^{n} M_j$
A
(3) $\widetilde{y} = sign(Dec(A))$
$\widetilde{y}$
(4) Here, $\widetilde{y} \neq y_1$
for $j = 1, \cdots, n$
$V_j = ex_{1,j}^{\eta}$
$ew_j^{(1)} = Enc(w_j^{(1)})$
$ew_j^{(2)} = ew_j^{(1)} \cdot V_j$
end for
$e\vec{w}^{(2)} = (ew_1^{(2)}, \cdots, ew_n^{(2)})$
(5) **for** $j = 1, \cdots, n$
$w_j^{(2)} = Dec(ew_j^{(2)})$
end for
$\vec{w}^{(2)} = (w_1^{(2)}, \cdots, w_n^{(2)})$
Repeats step (2)

Fig. 2. The Process of A Concrete Example

- Hospital: initializes a weight vector $\vec{w}^{(1)} = (w_1^{(1)}, \cdots, w_n^{(1)})$, sends it to the cloud server.
- Cloud server: chooses the medical case $e\vec{x}_1 = (ex_{1,1}, \cdots, ex_{1,n})$, calculates $M_j = ex_{1,j}^{w_j^{(1)}}$ (for $1 \leq j \leq n$) and $A = \prod_{j=1}^{n} M_j$, returns A to the hospital.
- Hospital: decrypts A and calculates $\widetilde{y} = sign(Dec(A))$, sends $\widetilde{y}$ to the cloud server.

– Cloud server: because $\widetilde{y} \neq y_1$, calculates $V_j = ex_{1,j}^{\eta}$ and $ew_j^{(1)} = Enc(w_j^{(1)})$ (for $1 \leq j \leq n$). And then, it calculates $ew_j^{(2)} = ew_j^{(1)} \cdot V_j$ (for $1 \leq j \leq n$) and sends back the ciphertext of updated weight vector $e\vec{w}^{(2)}$ to the hospital.
– Hospital: decrypts the ciphertext of updated weight $w_j^{(2)} = Dec(ew_j^{(2)})$ (for $1 \leq j \leq n$), suppose the number of iterations is less than a preset threshold, it sends the $\vec{w}^{(2)} = (w_1^{(2)}, \cdots, w_n^{(2)})$ to the cloud server.

Now, $\mathscr{A}$ possesses the plaintext of weight vector $\vec{w}^{(1)}$ before updating, the plaintext of updated weight vector $\vec{w}^{(2)}$, the learning rate η and the desired output y_1. Trivially, $\mathscr{A}$ can obtain the values of medical case $\vec{x}_1 = (x_{1,1}, \cdots, x_{1,n})$ according to the linear equation with one unknown number $\vec{w}_j^{(2)} = \vec{w}_j^{(1)} + \eta y_1 \vec{x}_{1,j}$ (for $1 \leq j \leq n$). Therefore, the cloud server can obtain the private medical information $\vec{x}_1$ by solving these equations. Furthermore, the more times the algorithm iterates, the more medical cases will be leaked.

4 Conclusion

In this paper, we present that the PSLP scheme proposed by Wang et al. [3] is not secure against the honest-but-curious cloud server. The reason why their scheme suffers from the serious attack is that in paillier cryptosystem the cloud server must obtain the plaintext of weight vector to calculate the product $\vec{w} \cdot \vec{x}_i (i \in \{1, \cdots, m\})$, which leads to the cloud server obtain the plaintexts of the medical cases easily by the equation $\vec{w} = \vec{w} + \eta y_i \vec{x}_i$. Therefore, the PSLP scheme can not protect the sensitive medical information as they claimed. And we will give a full solution in our future works.

References

[1] Xindong Wu, Xingquan Zhu, Gong-Qing Wu, and Wei Ding. Data mining with big data. *ieee transactions on knowledge and data engineering*, 26(1):97–107, 2014.

[2] Wei Fan and Albert Bifet. Mining big data: current status, and forecast to the future. *ACM sIGKDD Explorations Newsletter*, 14(2):1–5, 2013.

[3] Guoming Wang, Rongxing Lu, and Cheng Huang. Pslp: Privacy-preserving single-layer perceptron learning for e-healthcare. In *Information, Communications and Signal Processing (ICICS), 2015 10th International Conference on*, pages 1–5. IEEE, 2015.

[4] Fanyu Bu, Yu Ma, Zhikui Chen, and Han Xu. Privacy preserving back-propagation based on bgv on cloud. In *High Performance Computing and Communications (HPCC), 2015 IEEE 7th International Symposium on Cyberspace Safety and Security (CSS), 2015 IEEE 12th International Conferen on Embedded Software and Systems (ICESS), 2015 IEEE 17th International Conference on*, pages 1791–1795. IEEE, 2015.

[5] Qingchen Zhang, Laurence T Yang, and Zhikui Chen. Privacy preserving deep computation model on cloud for big data feature learning. *IEEE Transactions on Computers*, 65(5):1351–1362, 2016.