Collaborative Learning Using Optical Back Propagation Neural Network Over Cloud Computing

Dhayalan.D
Assistant Professor, Department of MCA, Vel Tech High Tech Dr.Rangarajan Dr.Sakunthala Engineering College, Avadi-600 062, India

Jeevitha.R
PG Scholar, Vel Tech High Tech Dr.Rangarajan Dr.Sakunthala Engineering College, Avadi-600 062, India

***Abstract*—**To improve the accuracy of learning result in practice multiple parties may collaborate through conducting joint propagation neural network learning on the union of their respective data sets. In this process no party wants to disclose the private data to others. Back-propagation supporting this kind of collaborative learning takes long time to converge and may fall into local minima. One of the possible techniques to escape from local minima is by using a very small learning rate which will slow down the learning process. And can be solved by using "Optical Back-Propagation" algorithm which escapes from local minima with high speed of convergence during the training period. During this process it allows two or more parties with an arbitrarily partitioned data set to conduct the collaborative learning. In cloud computing each party encrypts the private data locally and uploads the cipher text to the cloud then the cloud executes most of the operation pertaining to the learning algorithm over cipher text without knowing the original private data. We keep the computation and communication cost on each party minimal and independent to the number of participants by using secure operations on the cloud. We use doubly homomorphism encryption algorithm for multiparty setting to support flexible operation over cipher texts. This shows that our scheme is secure, flexible and accurate.

***Keywords*—**Back-Propagation, Cloud Computing, Neural network, Optical Back-Propagation, Privacy preserving.

I. INTRODUCTION

Back-Propagation is an effective method for learning neural networks and has been used in various applications such as health care, disclosure of sensitive information and for business purpose. To improve the Internet-wide collaborative learning it is imperative to provide a solution that allows the participants to conduct neural network learning jointly without disclosing their respective private data sets. The solution shall be efficient and scalable to support arbitrary number of participants. To provide solutions for privacy preserving back-propagation neural network learning we use BGN doubly homomorphism encryption algorithm in which each participant first encrypts the private data with systems public key and then uploads the cipher text to the cloud, the cloud servers then execute most of the operations pertaining to learning process over the cipher text and return the encrypted results to the participants then the participants jointly decrypt the results. This paper provides privacy preserving for multi party collaborative back-propagation neural network learning over arbitrary portioned data. The main idea of our scheme is the ability to escape from local minima with high speed of convergence during the training period. However in some cases the standard back-propagation neural network takes unendurable time to adapt the weights between the units in the network to minimize the mean squared errors between the desired output and actual network output .There has been proposed to improve this algorithm by using non linear functions which applied to an output units. The convergence speed of learning process can be improved significantly by "optical back-propagation" through adjusting the error which will be transmitted backward from the output layer to each unit in the intermediate layer.

II. STANDARD BACK PROPAGATION

The standard back-propagation neural network takes unendurable time to adapt the weights between the units in the network to minimize the mean squared errors between the desired output and actual network output. Fig 1 represent the back-propagation learns predefined set of output after an input pattern has been applied to the first layer of network unit it is propagated through each upper layer until an output is generated. This output pattern is then compared through desired output and the error signal is computed for each signal unit. The signals are then transmitted backward from the output layer to each unit in the intermediate layer that contributes directly to the output. Each unit in the intermediate layer receives only a portion of total error signal based roughly on relative contribution the unit made to output. This process repeats layer by layer until each unit in the network has received an error signal that describes its relative contribution to total error. There has been proposed to improve this algorithm by using non linear functions which applied to output units. The convergence speed of learning process can be improved significantly by optical back-propagation through adjusting the error which will be transmitted backward from the output layer to each unit in the intermediate layer.

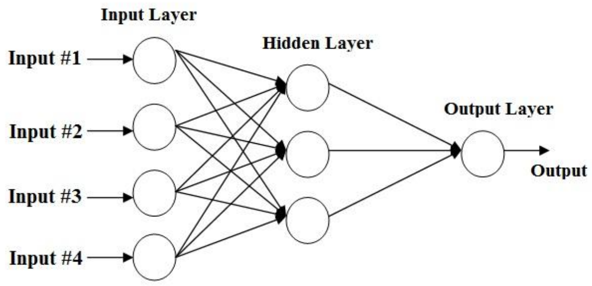


Fig 1. Configuration of back propagation

III. OPTICAL BACK PROPAGATION

The new algorithm optical back propagation will be described at which it would improve the performance of the back propagation algorithm. The convergence speed of the learning process can be improved significantly by optical back propagation through adjusting the error which will transmit backward from the output layer to each unit in the intermediate layer.

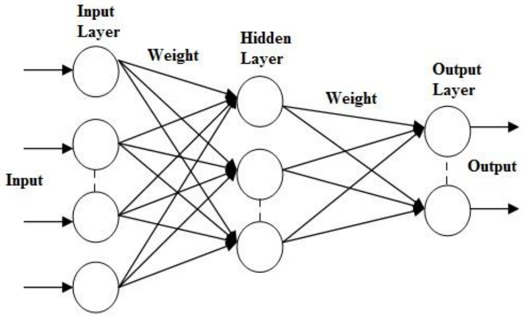


Fig 2. Configuration of optical back propagation

In back-propagation the error at single output unit is defined as:
To propagate output which updates the outer-layer weights and the hidden-layer weights is equal to the difference between desired output value of trained vector and output unit of actual output from trained vector and output unit.

While the error at single output unit in adjusted between optical back-propagation neural network will be defined as:
An optical back-propagation neural network uses two forms to propagate output which update the outer-layer weights and the hidden-layer weights because the exp function always returns zero or positive values. This new method will minimize the error
s of each output unit more quickly than the old back-propagation method and the weights on certain units change very large from their starting values. The Fig 2 represents the Optical back-propagation.

A. Steps Of Optical Back-Propagation

1. Apply the input to the input units.
2. Calculate the net-input values to the hidden layer units.
3. Calculate the outputs from the hidden layer.
4. Calculate the net-input values to the output layer units.
5. Calculate the outputs from the output units.
6. Calculate the error term for the output units but replace new optical back-propagation with standard back-propagation.
7. Calculate the error for the output units using new optical back-propagation method also,
8. Update weights on the output layer.
9. Update weights on the hidden layer.
10. Repeat the steps 1 to step 9 until the error is acceptably small for each training vector pairs.

B. Proof

In Back Propagation the error at single output unit is defined as:

$$\delta^\circ_{pk}=(Y_{pk}-O_{pk}) \qquad (1)$$

Where “p” refers to the training vector, and “k” refers to the output unit. In this Y_{pk} is the output value, and O_{pk} is the actual output from k unit, then δ°_{pk} will propagate backward to update output layer weights and the hidden layer weights.
The error at single output unit in adjusted Optical Back Propagation will be:

$$New\delta^\circ_{pk}= (1+ e^{(Y_{pk}-O_{pk})^2}) \qquad (2)$$

,if $(Y_{pk} - O_{pk})$>=ZERO.

$$New\delta^\circ_{pk}=- (1+ e^{(Y_{pk}-O_{pk})^2}) \qquad (3)$$

,if $(Y_{pk} - O_{pk})$<ZERO.

WhereNewδ°_{pk} is considered asproposed in Optical Back Propagation algorithm.

Optical Back Propagation uses two forms of Newδ°_{pk}because the execution function always returns zero or positive values. This Newδ°_{pk} will minimize the errors of each output unit more quickly than the old δ°_{pk} and the weights on certain units change very large from their starting vales.

Theoutput of Back Propagation and Optical Back Propagation for output unit must be equal if the Back Propagation output units multiply it by factor(A) where (A) is defined as:

$$A.1 / 1+e^{-x}=(1+ e^{(Y_{pk}-O_{pk})^2}) \qquad (4)$$

$$A=(1+ e^{(Y_{pk}-O_{pk})^2}\ )\ 1+e^{-x} \qquad (5)$$

The sigmoid function for each output in BP must be equal to the Newδ°_{pk} in OBP through multiplying it by this Factor.
There is another way to find the factor (A) using the following assumptions:

Assumption 1:

$$A\,.\,1/\,1+e^{-x}=1/\,(1+e^{Y_{pk}-O_{pk}}) \tag{6}$$

In this ,OBP uses a sigmoid function on each error of each output unit and it assumes if sigmoid function is multiplied by (A1) it must be equal to those sigmoid functionwhich applied on the error for output units.

$$A1=\ 1+e^{-x}/(1+e^{Y_{pk}-O_{pk}}) \tag{7}$$

Assumption 2:

OBP assumes that if the sigmoid function is applied on the error of output units is multiplied by (A2) then it must be equal to $New\delta^{\circ}_{pk}$.

$$A2.1/\,(1+e^{Y_{pk}-O_{pk}})=(1+e^{(Y_{pk}-O_{pk})^2}) \tag{8}$$

$$A2=(1+e^{Y_{pk}-O_{pk}})(1+e^{(Y_{pk}-O_{pk})^2}) \tag{9}$$

Assumption 3:

From equations (7) and (9) OBP assumes as:

$$A= A1*A2 \tag{10}$$

$$A=1+e^{-x}/(1+e^{Y_{pk}-O_{pk}})(1+e^{Y_{pk}-O_{pk}})(1+e^{(Y_{pk}-O_{pk})^2}) \tag{11}$$

$$A=(1+e^{-x})(1+e^{(Y_{pk}-O_{pk})^2}) \tag{12}$$

IV. SYSTEM MODEL

We consider a system composed of three major parties trust agent, the participating party and the cloud server. Trust agent is the party responsible for generating and issuing encryption and decryption keys for all the other parties which will not participate in any computation other than key generation and issuing. Each participating party owns the private data sets and wants to perform collaborative optical back-propagation network learning with all other participating parties. That is it will collaboratively conduct learning over the arbitrarily partitioned data set which is private and cannot be disclosed during the learning process that each participating party stays online with broadband access to the cloud and is equipped with one or several contemporary computers which can work in parallel if there are more than one.

V. SECURITY MODEL

The existence of Trust agent who is trusted by all parties will have the knowledge of system secret key and will not participate in any computation besides the key generation and issuing. Trust agent is allowed to learn about each party's private data whenever necessary. The existence of Trust agent is useful when investigation is needed in case some malicious party intentionally interrupts the system. In real life parties such as the government agents or organization alliances can be the Trust agent. The participating party does not fully trust each other and they do not want to disclose their respective private data to any other parties than Trust agent except for the final weights learned by the network.

VI. ARBITRARY PARTITIONED DATA

In privacy preserving optical back-propagation neural network algorithm when training data for the neural network is arbitrarily partitioned between two parties both parties want to train the network at the same time no party is able to learn anything about other party data except the final weights learned by the network. In this both parties modify the weights and hold random shares of the weights during the training.

VII. PRESERVING NEURAL NETWORK LEARNING

In privacy preserving optical back-propagation neural network learning after training both the parties holds the random shares of weights and not the exact weights this guarantees more security and privacy against the intrusion by the other party. It is the only at the end of the training that both the parties know the actual weights in the neural networks. The aim of this algorithm is to train the network to modify the weights so that given input distributed data set between the parties the output corresponds nearly to the target value. At the end of training each party holds only a random share of each weight.

VIII. CLOUD COMPUTING

Cloud computing provides a hub of resources and computation power to the client of services are delivered through internet. Cloud computing is a model for enabling convenient on-demand network access to a shared pool of configurable computing resources like networks, server, storage, application and services that can be rapidly provisioned and released with minimal management effort or service provider interaction. Cloud computing consists of four models private, community, public and hybrid cloud.

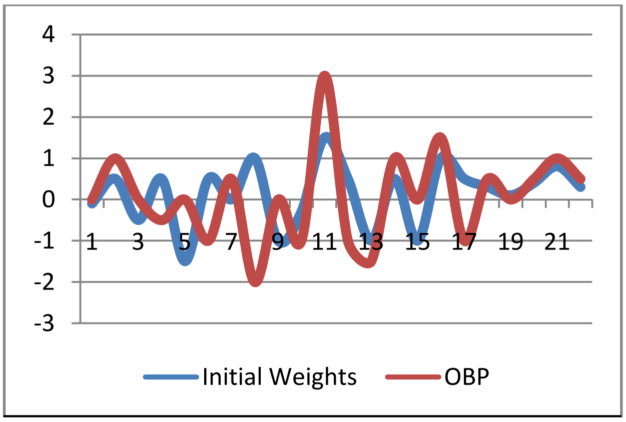
Cloud computing can be divided into categories like:

1) Cloud platform: This is related to possible virtualization, storage and network vulnerabilities.
2) Data: This relates to integrity of data, confidentiality of data and privacy of user.
3) Access: This relates about the cloud access like authentication, authorization.
4) Compliance: The size and disruptive influence of the cloud is attracting attention from security auditing, data location, operation traceability and compliance.

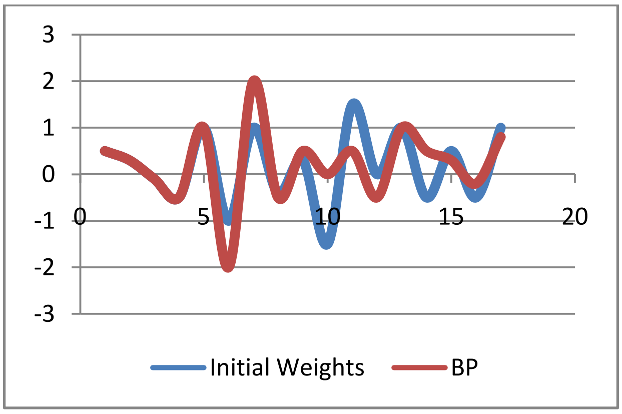
To ensure data integrity in cloud data need to be protected using strong encryption mechanism like doubly homomorphism encryption. Homomorphism encryption is gaining increased attention from various perspectives as cloud computing has become popular and changing the way people use technology to deal with their data. Homomorphism encryption preserves the structure of two objects operated on by the same arithmetic operations. Such a characteristics make homomorphism encryption one of the most suitable encryption for enabling data in cloud storage to be processed in its encrypted form.

IX. COMPARITIVE STUDY OF OBP AND BP

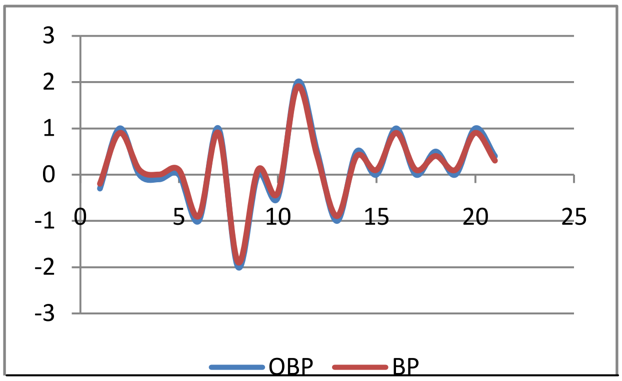
The back-propagation and optical back-propagation neural network can be compared with input, hidden and output layer with respect to weights. The Fig 3 and Fig 4 represent the Final weight values from input to hidden and hidden to output. First train thenetworks using optical-back propagation then it trains using standard back propagation and finally it compares the final results from optical back propagation and standard back propagation. Training process defined as adapting weights of each unit of neural network. Thus optical back-propagation can adapt all weights with optical time and the simulation result shows that when a very small values used for learning rate with optical back propagation makes the adapted final weights very closed become the final weights from back-propagation. Finally it escapes from local minima.



(a) Adapting process of weights from input to hidden layer using OBP

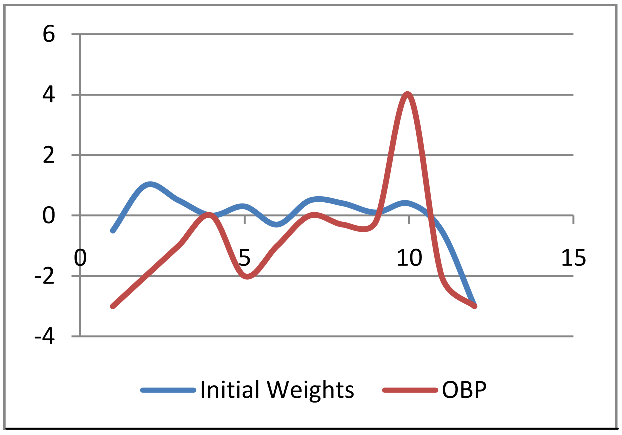


(b) Adapting process of weights form input to hidden layer using BP

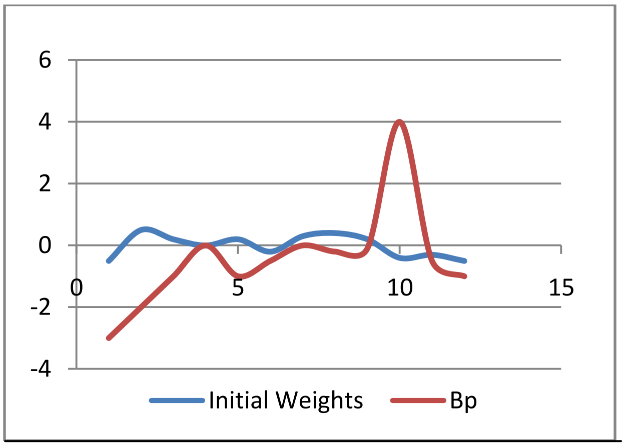


(c) Final weights using the BP and OBP

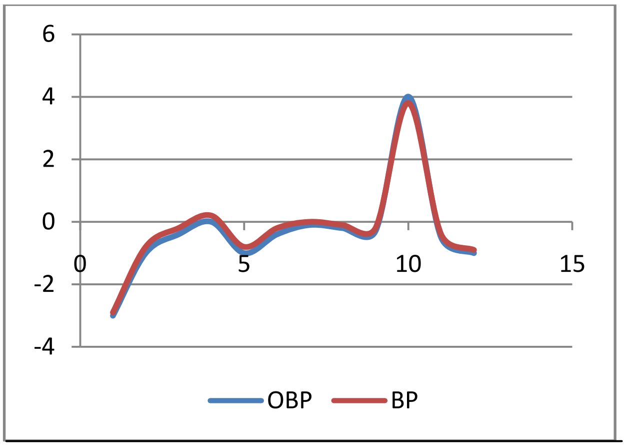
Fig 3. Final weight values from input to hidden



(a) Adapting process of weights from hidden to output layer using OBP



(b) Adapting process of weights from hidden to output layer using BP



(c) Final weights using the BP and OBP

Fig 4. Final weight values from hidden to output

Table 1 Training Processes using different weights

Learning Rate(Weight)	OBP	BP
0.01	1812	46798
0.05	363	9351
0.1	182	4673
0.15	122	3114
0.2	92	2334
0.25	47	1866
0.3	61	1554

X. CONCLUSION

In this work we proposed a optical back propagation neural network learning scheme over arbitrarily partitioned data. our proposed approach the parties encrypt their arbitrarily partitioned data and upload the cipher texts to the cloud so that the cloud can execute most operations pertaining to the optical back-propagation neural network learning algorithm without knowing any private information. And it is proposed for training multilayer neural network this shows that optical back-propagation neural network is beneficial in speeding up the learning process.

REFERENCE

[1] D. Asonov and J. Freytag. Almost optimal private information retrieval. In Proceedings of the International Conference on Privacy Enhancing Technologies (PET), pages 209-223, 2003.

[2] S. Bugiel, S. Nurnberger, A. Sadeghi, and T. Schneider. Twin clouds: Secure cloud computing with low latency. In Proceedings of the IFIP International Conference on Communications and Multimedia Security (CMS), pages 32-44, 2011.

[3] C. Yu, S.S.M. Chow, K. Chung, and F. Liu. Efficient secure two-party exponentiation. In Proceedings of the Cryptographers' Track at the RSA Conference Topics in Cryptology (CT-RSA), pages 17-32,2011.

[4] You-Jin, K.-Y. Park and J.-M. S. Kang, "The method of protecting privacy capable of distributing and storing of data efficiently for cloud computing environment," 2011 First ACIS/JNU International Conferenceon Computers, Networks, Systems and Industrial Engineering (CNSI), pp.258-262, 2011.

[5] C. Delettre, K. Boudaoud and M. Riveill, "Cloud Computing, Security and Data Concealment," 2011 IEEE Symposium on Computers andCommunications (ISCC), pp. 424-431, 2011.

[6] M. Barbosa and P. Farshim, "Delegatable Homomorphic Encryption with Applications to Secure Outsourcing of Computation," Cryptology ePrint Archive: Report 2011/215, pp. 1-29, 2011.

[7] M. Brenner, J. Wiebelitz, G. v. Voigt and M. Smith, "Secret ProgramExecution in the Cloud Applying Homomorphic Encryption," 2011Proceedings of the 5th IEEE International Conference on Digital Ecosystems and Technologies Conference (DEST), pp. 114-119, 2011.

[8] A. Sahai, "Computing on Encrypted Data," Springer-Verlag Berlin Heidelberg, pp. 148 - 153, 2008.

[9] D. Boneh, E.-J. Goh and K. Nissim, "Evaluating 2-DNF Formulas on Ciphertexts," Second Theory of Cryptography Conference, TCC 2005,Cambridge Proceedings, pp. 325-341, 2005.

[10] Q. Liu, GuojunWang and JieWub, "Secure and privacy preserving keyword searching for cloud storage services," Journal of Network and Computer Applications, vol. 35, no. 3, pp. 927-933, 2012.

[11] Barni, M., Orlandi, C., &Piva, A. (2006). A Privacy-Preserving Protocol for Neural-Network-Based Computation, in Proceeding of the 8th workshop on Multimedia and security. 146-151.

[12] Chen, T., &Zhong, S., (2009). Privacy Preserving Back-Propagation Neural Network Learning, IEEE Transactions on Neural Networks, 20(10) 1554 - 1564.