ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2015

A Survey on Privacy Preserving Neural network with Cloud computing

Rashmi Nade [1], Prof.P.D.Lambhate [2]

P.G. Student, Dept. of Computer Engineering, JSCOE, Handewadi Road, Pune, India[1]

Associate Professor, Dept. of Computer Engineering, JSCOE, Handewadi Road, Pune, India[2]

ABSTRACT: During the collaborative learning of neural network on cloud computing, multiple parties collaborate with their own private data sets. As the collaborative neural network learning process starts a individual data sets of all parties are collected and during this learning process no party needs to disclose her/his non-public information to others. The existing methods that support this kind of approach for collaborative learning, but these are limited only for two parties as well as data partition. There is no solution for two or more parties, for collaboratively conduct the learning, with an arbitrarily partitioned data set. Here is a solution presented to overcome the above stated limitations of existing collaborative learning methods used in cloud computing. This open problem is solved by using the power of cloud computing. In this proposed scheme, each party encrypts his/her private data locally and uploads the encrypted data which is cipher texts into the cloud. Then cloud executes most of the operations pertaining to the learning algorithms over cipher texts without knowing the original private data. Back Propagation algorithm is used for learning the neural network

KEYWORDS: Neural Network, Cloud Computing, Back Propagation, Privacy Preserving.

I. INTRODUCTION

Neural Network is formed with a set of inputs and outputs units which are connected, and each connection has a weight associated with it. Neural Network has three main layers, first is Input layer which consist a values of data record and these values are input to next layer, Second is middle layer or hidden layer, there are many hidden layers and Third layer is Output layer. To learn the neural networks back propagation and feed forward are the two methods, but the back propagation is a very popular and effective method. This is widely used in various applications, like character recognition, image compression, stock market prediction, traveling salesman problem, weather prediction.

Back propagation method works backward, it calculates the error between output (expected values) and calculated values and trains neural network until the results are near to expected values. For training a neural network we need a training data set, which is very important because correctness of the learning result depends on data. When we use the high quality data results are better. So instead of learning on local data set we do collaborative learning. In collaborative learning multiple parties are involved with their private data sets; parties included in collaborative learning can use the data sets of other parties also. For such learning process cloud computing is the best computing infrastructure.

Cloud is an infrastructure which provides resources and services over the internet. Cloud computing platform gives a large computing capacity; capacity is resizable in the cloud. By using the cloud we can save the time and application can develop and deploy faster.

As we know in collaborative learning multiple parties include with their private data sets, and during the learning process data is collected by each party, so we must provide a protection to their private data sets because no one wants to disclose their private information to any other.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2015

In many applications protection of private data is a legal issue like Health Insurance Portability and Accountability Act (HIPAA). It is very important as the private data of user in very sensitive.

By taking in consideration all above things, we need to provide a solution which allows all participants to conduct a collaborative neural network learning process without revealing their respective private data sets. So, to provide a practical solution for conducting privacy preserving back propagation neural network learning process (this is the process which is used to train the neural networks) we need to concentrate on some important things these are as follows:

At first it is important that during learning process when the data is collected it should not be in plaintext format, it should be in encrypted format. So that during the processing private data of user is protected and the in between results also, in between results contains sensitive information so we need to protect this. This can be achieved by secure computation of various operations like addition, scalar product and the nonlinear sigmoid function, which are used by the BPN network algorithm.

The cost required for proposed solution, which is communication/computation cost shall be affordable for each participant. Scalability of system should be considered, so that arbitrary number of participants can take part in learning process.

The data sets in collaborative learning should be partitioned arbitrarily not by a single way.

II. RELATED WORK

Various privacy preserving BPN network learning methods have been proposed in the last few days. These are as follows:

Jiawei Yuan; Shucheng Yu. "Privacy Preserving Back-Propagation Neural Network Learning Made Practical with Cloud Computing,"[1]

Here a back propagation neural network learning algorithm is used for learning process over arbitrarily partitioned data. As we discussed above back propagation method is very efficient for training neural networks and here data is arbitrarily partitioned means here is no limitations for partitioning data like data is partitioned only horizontally or only vertically, it can be portioned either horizontally or vertically.

Here a solution is proposed for multiple parties, so the protection of each users private data is very important task, for this purpose they have implemented a privacy preserving multiparty BPN network learning algorithm.This method protects the private data of participants and also protects the in between results produced during the process of learning. To protect the learning result a secure scalar product algorithm is used.

This System has three main parties:

Trusted authority (TA): which is responsible for generating private and public keys, where public key is used to encrypt the users private data and private key is used to decrypt the data. TA have access to learn any private data.

Participating parties (data owner): Each participating party has its own private data set and wish to perform collaborative neural network learning with other parties.

Cloud servers (or cloud): Gives platform for the participating parties. Here it is assumed that all parties stay online with access to cloud

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2015

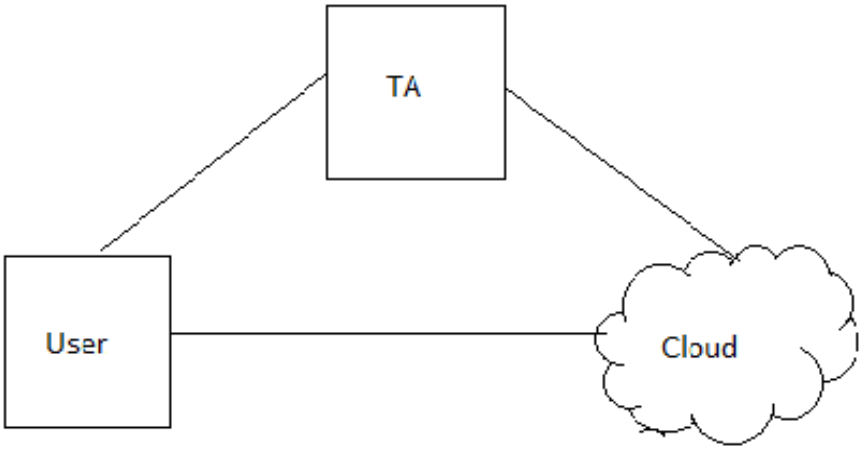

Fig. 1 System Flow

System flow

1. User encrypts his/her private data by using the keys generated by Trusted authority.
2. The Encrypted data is uploaded to cloud .
3. Cloud stores the data uploaded by users, As data is encrypted it is not understandable by any parties.
4. Cloud apply Neural Networking on data, Here the neural network is trained by BPN algorithm. During the training intermediate results are not revealed.
5. A final weights are generated.

N. Schlitter. "A protocol for privacy preserving neural network learning on horizontal partitioned data". [3]

This paper also gives a method for privacy preserving BPN network learning, and allows two or more than two parties to jointly conduct Back Propagation Neural network learning. During this process private data of users does not revealed. As this method allows more than two parties, it needs a secure sum and secure matrix addition so for this purpose a neural network classification algorithm is used , this algorithm is extension of Rumelhart's clasification algorithm. Here are some limitations, that the solution is given only for horizontal partitioned data, in horizontal partitioning of data every user share the same data schema, and each party holds some records of total data sets.This method uses a extension of Rumelheart algorithm which does not guarantee privacy.This method cannot protect, in between results, generated during the BPN learning process. To protect the private data of participants, a secure computation of in between results is very important, because in between results also contains the sensitive data.

T. Chen and S. Zhong. " Privacy-preserving backpropagation neural network learning."[2]

This paper presents a privacy preserving BPN network learning algorithm, but this algorithm is applicable only for two parties. This algorithm provides a strong security for data sets and during the learning process it protects the in in between results. This method is having drawbacks like it just supports two parties. This method only supports vertically partitioned data. This method is not scalable.

A. Bansal, T. Chen, and S. Zhong. "Privacy preserving backpropagation neural network learning over arbitrarily partitioned data."[7]

This paper presents a improved method and gives a solution for data which is arbitrarily partitioned. In arbitrary partitioning of data, there is no order of how the data is divided. This method is just like the method used in [2],

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2015

which was for vertically partition of data, and here it is for arbitrary partition of data. Here they tried to extent the method from two party to multi party scenario But, extension of two party to multi party introducesa computation/ communication complexity which is quadratic in the number of participants. In real world implementation, such a complexity represents a huge cost on each party. That's why this paper just considers the two-party scenario though it supports arbitrarily partitioned dataset.

By studying the above papers we came to know that none of existing system solved the problems at same time. There still lacks a efficient and scalable solution that supports a collaborative BPN learning with privacy preserving, over arbitrary partitioned data

III. CONCLUSION

The cloud computing platform used in privacy preserving minimizes the communication cost and computation cost. Here a cost of each party is not dependent on any other participating parties. A privacy preserving multiparty BPN network learning algorithm used to secure the data of all users. This scheme is secure, efficient and scalable. A future work is to prepare a multiuser collaborative learning without the help of TA (trusted authority), and try to minimize the communication, computation cost.

REFERENCES

[1] Jiawei Yuan; Shucheng Yu. "Privacy Preserving Back-Propagation NeuralNetwork Learning Made Practical with Cloud Computing," *IEEE Transaction paper on parallel and distributedsystem, digital object identifier* 10.1109/TPDS.2013.18,1045-9219/13/$31.00,2013 IEEE.

[2] T. Chen and S. Zhong. "Privacy-preserving backpropagation neural network learning". *Trans. Neur. Netw.*, 20(10):1554–1564, Oct. 2009.

[3] N. Schlitter. "A protocol for privacy preserving neural network learning on horizontal partitioned data". In *Proceedings of the Privacy Statistics in Databases (PSD)*, Sep. 2008.

[4] D. Boneh, E.-J. Goh, and K. Nissim. "Evaluating 2-dnf formulas on ciphertexts". In *Proceedings of the Second international conference on Theory of Cryptography*, TCC'05, pages 325–341, Berlin, Heidelberg,2005.

[5] A. Frank and A. Asuncion. "UCI machine learning repository", 2010.

[6] A. Bansal, T. Chen, and S. Zhong." Privacy preserving backpropagation neural network learning over arbitrarily partitioned data". *Neural Comput. Appl.*, 20(1):143–150, Feb. 2011.