IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 7, July 2017

Privacy Preserving Back-Propagation Neural Network Data Security in Client and Server

C. Amirtha Rani[1]

Asst Prof, Computer Science Department, Syed Ammal Arts and Science College, Ramanathapuram, Tamil Nadu[1]

Abstract: Now-a-days there is lots of security that promises to provide excellent security, but in spite of that many of them fail to deliver when it comes to real time testing. Each authorized party easily identified the data and message. We use the many ways needed to prevent. So encrypt all data and message only use the authority person knowing the data and message. One or more persons communicate and the computation of participants. So secure the data and message very secretly. To prevent use neural network methods every data give the secret key and give some weighted also when it sends the message to the server. In this paper, we present a privacy preserving algorithm for the neural network learning, when the dataset in arbitrary partitioned between the two parties. We show that our algorithm in very secure and leak no knowledge about the other part's data. We demonstrate the efficiency of our algorithm by experiment on real world data. The computation and communication costs on each party minimal and independent to the number of participants. To support flexible operations over cipher texts, Numerical analysis and experiments on commodity show that our scheme is secure, efficient and accurate. The neural networks are distributed between two parties, which are quite common nowadays. Existing cryptographic approaches such as secure scalar product protocol provide a secure way for neural network learning when the training data set is vertically partitioned. In this algorithm after each round of training both the parties just hold the random shares of weights and not the exact weights, this guarantees more security and privacy against the intrusion by the other party.

Keywords: Back Propagation, Neural network, Data Security, Client and Server.

I. INTRODUCTION

Back propagation [1] is an effective method for learning, neural networks and has been widely used in various applications. The accuracy is highly affected by the volume of high quality data. The participating parties carry out learning not only on their own data sets, but also on others' data sets. It has been more convenient than ever for users across the Internet, who may not even know each other to conduct joint collaborative learning through the shared infrastructure. Neural Network is composed of highly interconnected processing element called Neuron. This is having a limited number of input and output. Designing or programmed this system for learning the recognize patterns. Learning can be supervised or unsupervised. In supervised learning there is a master to monitor the network learning activity where as in unsupervised learning there is no master for monitoring the learning.

The learning accuracy is mainly affected by the data used for learning. Instead of learning with limited dataset collaborative learning improves the learning result. Privacy preserving back-propagation neural (BPN) network learning, there are mainly three challenges:
1. Give protection to each participant's private dataset and intermediate results produced during the BPN network learning process. It requires secure computation of various operations.

II. RELATED WORK

Back Propagation Algorithm

Artificial Neural Networks (ANNs), Connectionism or Connectionist Models, Multi-layer Percpetrons (MLPs) and Parallel Distributed Processing (PDP). There is a small group of "classic" networks, which are widely used and on which many others are based. These are: Back Propagation, Hopfield Networks, Competitive Networks and networks using Spiky Neurons. There are many variations even on these themes.

The algorithm

Most people would consider the Back Propagation network to be the quintessential Neural Net. Actually, Back Propagation is the training or learning algorithm rather than the network itself. The network used is generally of the simple type in these are called Feed Forward Networks. The network operates in exactly the same way as the others we've seen. Now, let's consider what Back Propagation is and how to use it.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 7, July 2017

A Back Propagation network learns by example. You give the algorithm examples of what you want the network to do and it changes the network's weights so that, when training is finished, it will give you the required output for a particular input. Back Propagation networks are ideal for simple Pattern Recognition and Mapping [6]. As just mentioned, to train the network you need to give it examples of what you want – the output you want (called the Target) for a particular input as shown in Figure 1.1.

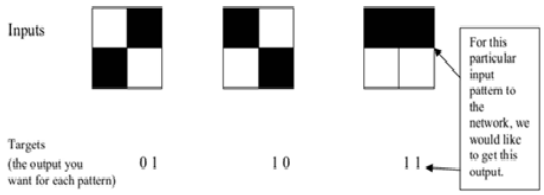

Figure 1.1, a Back Propagation training set.

So, if we put in the first pattern to the network, we would like the output to be 0 1 as shown in figure 1.2 (a black pixel is represented by 1 and a white by 0 as in the previous examples). The input and its corresponding target are called a Training Pair.

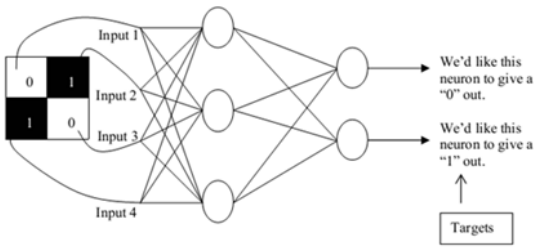

Figure 1.2 applying a training pair to a network.

Once the network is trained, it will provide the desired output for any of the input patterns. Let's now look at how the training works. The network is first initialized by setting up all its weights to be small random numbers – say between –1 and +1.

Next, the input pattern is applied and the output calculated (this is called the forward pass). The calculation gives an output which is completely different to what you want (the Target), since all the weights are random. We then calculate the Error of each neuron, which is essential: Target - Actual Output (i.e. What you want – What you actually get). This error is then used mathematically to change the weights in such a way that the error will get smaller. In other words, the Output of each neuron will get closer to its Target (this part is called the reverse pass). The process is repeated again and again until the error is minimal. Let's do an example with an actual network to see how the process works. We'll just look at one connection initially, between a neuron in the output layer and one in the hidden layer, figure 1.3.

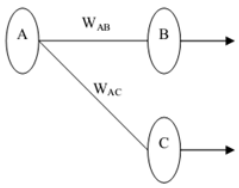

Figure 1.3 a single connection learning in a Back Propagation network.

The connection we're interested in is between neuron A (a hidden layer neuron) and neuron B (an output neuron) and has the weight W_{AB}.

The Algorithm Works like this:

First apply the inputs to the network and work out the output – remember this initial output could be anything, as the initial weights were random numbers.

2. Next work out the error of neuron B. The error is What you want – What you actually get, in other words:

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 7, July 2017

ErrorB= OutputB(1-OutputB)(TargetB– OutputB)

The "Output (1-Output)" term is necessary in the equation because of the Sigmoid Function – if we were only using a threshold neuron it would just be (Target – Output).

1.3 OBJECTIVE OF THESIS

To propose a privacy preserving algorithm for back-propagation neural network learning when the data is arbitrarily partitioned. Our contributions can be summarized as follows. This is the proposed privacy preserving for the neural networks when the data is arbitrarily partitioned. It is quite efficient in terms of computational and communication overheads. In terms of privacy, leaks no knowledge about other's party data except the final data's. To the best of our knowledge the problem of privacy preserving neural network learning over arbitrarily partitioned data has been solved
The main idea of this scheme can be summarized as follows: each participant first encrypts her/his private data with the system public key and then uploads the cipher texts to the server. Servers then execute most of the operations pertaining to the learning process over the cipher texts and return the encrypted results to the participants; the participants jointly decrypt the results with which they update their respective weights for the BPN network. During this process, cloud servers learn no privacy data of a participant even if they collude with all the rest participants. Provides privacy preservation for multi-party collaborative BPN network learning over arbitrarily partitioned data. To support multi-party secure scalar product and introduce designs that allows decryption of arbitrary large messages.

- There lacks a solution that allows two or more parties, each with an arbitrarily partitioned data set, to collaboratively conduct the learning.
- When the training data for the neural networks is arbitrarily partitioned between two parties, both parties want to train the network but at the same time they do not want that the other party should learn anything about its data except the final weights learned by the network. Limited in the way of data partition and Low performance.
- In such a case for neural network training this does not pose a significant privacy threat since each data holder can train the network in turns.
- Proposed System provides privacy preservation for multi-party (more than two parties) collaborative BPN network learning over arbitrarily partitioned data.
- Thorough analysis investigating privacy and efficiency guarantees of proposed scheme is presented real experiments on Amazon Server further show our scheme's several magnitudes lower computation /communicational costs than the existing ones.
- Support multi-party secure scalar product and introduce designs that allow decryption of arbitrary large messages. These improvements can be used as independent general solutions for other related applications.
- The present a privacy preservation back propagation neural network training algorithm when the training data is arbitrarily partitioned between two parties.
- The propose privacy preserving back-propagation neural network learning algorithm for the arbitrarily partitioned data between two parties. High Performance, Low limitation for data partitioning and high security.
- In arbitrary partitioning of data between two parties, there is no specific order of how the data is divided between two parties.

III.METHODOLOGY

4.2 Security Model

The existence of a trusted authority who is trusted by all the parties, trusted authority has the knowledge of system secrete key and will not participate in any computation besides the key generation and issuing.

Fig: 4.1 Providing Membership Authority (Generate key ID)

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 7, July 2017

name	field	id
Amirtha	STUDENT	172
prakash	STUDENT	150
doss	EPLOYEE	116
amir	STUDENT	13
prakash12	EMPLOYEE	97
[psakdfs	STUDENT	113
anith	EMPLOYEE	198

Table: 1 Generate Authorized ID Number

4.2 Encryption of Data

Homomorphic property is properties of certain encryption algorithms where specific algebraic operation (multiplication) can be performed on plain text by performing the operations on encrypted message without actually decrypt them. The authorized user to send the files to the server. The entire files store in database.

Fig 4.2: Secure Data processing (File Encrypt)

4.3 Data Extraction

The data set extraction module can be used to extract the data set and it will be stored in the database for future use the data set was selected, after that it will be split separate data and it can be stored in the table to the user database. The every authorized user given identifies numbers.

4.4 System Model

A system composed of three major parties a trusted authority, the participating parties and the server. Trusted authority is the party only responsible for generating and issuing encryption/decryption key for all the other parties.

Draw nodes:

When send the file to the server given to the weighted nodes. Actually to give the wanted how many ways to the path which that nodes put the column of number of nodes show fig:4.3.

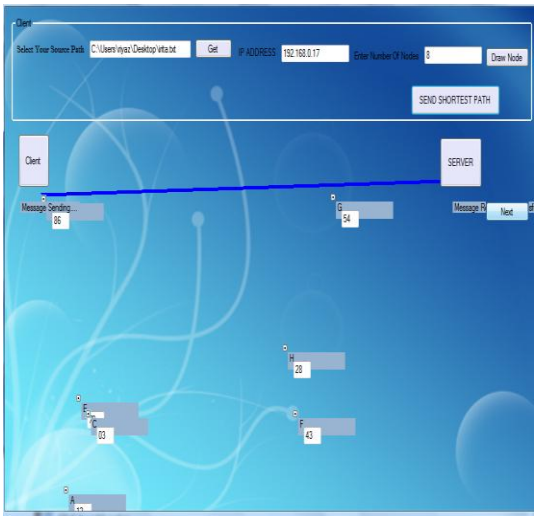

Fig 4.3: Weighted Nodes with Shortest path

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 7, July 2017

Segmentation:
The entire file sends to the server in the segmentation of the file. Segmentation the particular file in the service time in the database.

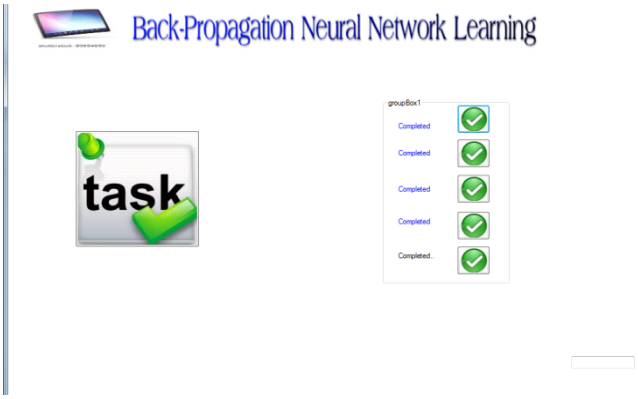

Fig 4.4: Segmentation of File

Show the service time and analysis of the time delay.

Fig 4.5: Service Time

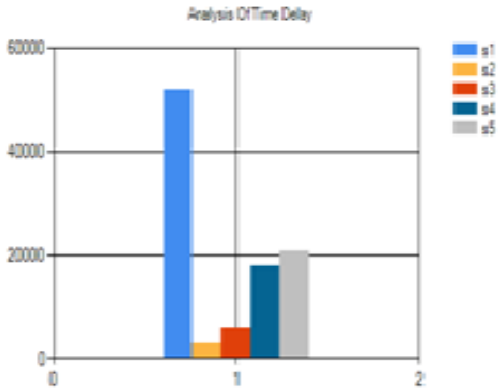

Fig 4.6: Time Delay

4.5 Result and Experimentation
To provide the experimental results after verifying the ID and decrypt the particular file. Result and decrypt the final learning result remain the same in the proposed scheme.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 7, July 2017

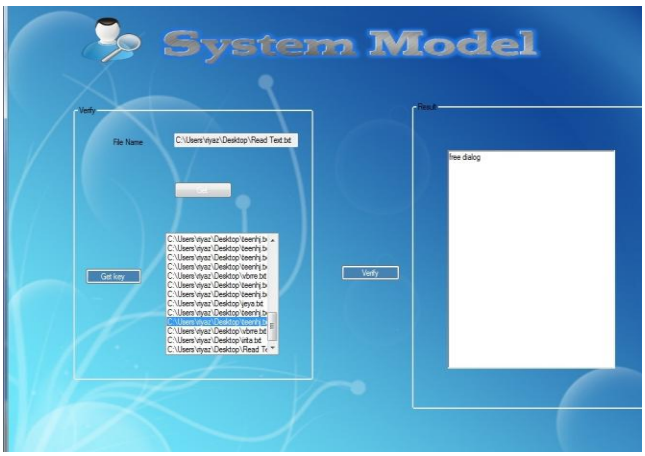

Fig 4.7: Experimentation of Result

IV. CONCLUSION

The proposed the first secure and practical multi-party BPN network learning scheme over arbitrarily partitioned data. In our proposed approach, the parties encrypt their arbitrarily partitioned data and up-load the cipher texts to the server. The server can execute most operations pertaining to the BPN network learning algorithm without knowing any private information. The cost of each party in our scheme is independent of the number of parties. The present a privacy preservation back propagation neural network training algorithm when the training data is arbitrarily partitioned between two parties. To assume a semi-honest model and our algorithm are quite secured as the intermediate results are randomly shared between the two parties. The experiments we perform on the real world data show that the amounts of accuracy losses are within limits.

REFERENCES

1. Agrawal, D., & Srikant, R. (2000). Privacy preserving data mining, InProc. ACM SIGMOD, 439-450.
2. Barni, M., Orlandi, C., & Piva, A. (2006). A Privacy-Preserving Protocol for Neural-Network-Based Computation, in Proceeding of the 8thworkshop on Multimedia and security. 146-151.
3. A. Bansal, T. Chen, and S. Zhong. Privacy preserving back propagation neural network learning over arbitrarily partitioned data. Neural Comput. Appl., 20(1):143–150, Feb. 2011.
4. Boneh.D Goh.E-J and K.Nissim Evaluating 2 dnf formulas on cipher texts. In proceeding of the second international conference on theory of cryphotography. Pages 325-341.
5. Charu .C Aggarwal , Tarek Abdolzaher, Integrating sensors and social network.
6. T. Chen and S. Zhong. Privacy-preserving backpropagation neural network learning. Trans. Neur. Netw., 20(10):1554–1564, Oct. 2009.
7. Di Vimercali S.D.C, S.Forest, S.Jajodia, S. para boschi and S.Samarali in the paper over encryption.
8. Flouri.K B.Berferull=Lozano, and p.Tsakalides in the paper training asvm based classifier in distributed sensor networks.
9. T.ELGamal in the paper "A public key cryptosystem and a signature scheme based on discrete algorithms".
10. Law.R in the paper "Back propagation in improving the accuracy of the neural network based tourism demand forecasting".