IJRRECS/March 2016/Volume-4/Issue-3/5206-5211 **ISSN 2321-5461**

INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE

DESIGNING OF AN EFFICIENT APPROACH FOR COMPUTATION OF NEURAL NETWORKS

G.Chandana Swathi[1], T.Geetha Lakshmi[2]

[1]Assistant Professor, CSE Dept, Santhiram Engineering College, Nandyal, A.P, India

[2]Assistant Professor, CSE Dept, Ellenki College Engineering and Technology, Hyderabad, T.S, India

ABSTRACT:

Recent studies from web users conclude that most of the people are worried regarding releasing of their private data to others. When there is distributed data in support of machine learning, privacy measures are necessary. The difficulty of privacy preserving neural network learning above arbitrarily partitioned information was not solved. We suggest a privacy preserving algorithm in support of back-propagation neural network learning when data is partitioned in the arbitrary way. The proposed algorithm is the first to suggest privacy preserving algorithm in support of neural networks when data is arbitrarily divided and it is relatively proficient regarding computational as well as communication overheads. Regarding privacy, our algorithm leaks no information regarding other's party information except final weights that are learned by network training end.

Keywords: Private data, Machine learning, Privacy preserving, Back-propagation Neural network learning, Arbitrary way.

1. INTRODUCTION:

With the development of Novel methods in databases or else in any other networks, solving of privacy issues has turn into an important problem. While all sorts of data are gathered from different sources, machine learning is uniformly increasing and hence are the issues concerning privacy. Neural Networks was been an active area of research for many years [1]. Trained neural networks can estimate resourceful outputs

which may be tricky to find in actual world. Existing methods of cryptography provides an efficient means for neural network learning when training dataset is partitioned in vertical means. The datasets which are used for training of neural network is collectively observed as virtual database. In distributed data situation this database is divided in lots of ways. When several rows of database are by single party and other party holds rest of rows of database, it is known as horizontal partitioned database and in such a situation for neural network training this does not cause a major privacy risk. When several columns of database are by one party and other party includes rest of columns, it denotes vertical partitioning of datasets intended for training. In our work we make a consideration of arbitrary partitioning of data among two parties in which there is no particular order of how data is separated among two parties. In our work we present an algorithm of privacy preserving for neural network learning when dataset is randomly partitioned among the two parties.

2. METHODOLOGY:

Training neural network from distributed information is common. During training of neural network from distributed data, confidentiality is an important issue and trained neural networks will assess resourceful outputs which might be difficult to find. Chen and Zhong has introduced algorithm of privacy preserving within neural networks when training data is partitioned vertically [2][3]. Vertically partitioned data for training is denoted when several columns of database are by one party and other party includes rest of columns. Their algorithm is resourceful and present tough privacy assurance. In our work we suggest a privacy preserving algorithm in support of back-propagation neural network learning when data is partitioned in the arbitrary way. Our work is the first to suggest privacy preserving algorithm in support of neural networks when data is arbitrarily divided. It is relatively proficient regarding computational as well as communication overheads. Regarding privacy, our algorithm leaks no information regarding other's party information except final weights that are learned by network training end. In our work we make a consideration of arbitrary partitioning of data among two parties. In the arbitrary data partitioning among two parties, there is no particular order of how data is separated

among two parties. When training information for neural networks is arbitrarily divided among two parties, these parties train the network but simultaneously they do not wish that other party have to study anything regarding its information apart from final weights that are learned by network. Hence we present an algorithm of privacy preserving for neural network learning when dataset is randomly partitioned among the two parties. It is extremely significant that not only data but intermediate weights moreover must not be exposed to other party since intermediate weights hold partial information regarding the data. We recommend an algorithm where both parties change weights and include random shares of weights throughout training. Both parties make use of secure two-party computation to compute random shares of weights among training rounds. In our work we imagine semi-honest representation which is a principle security representation in lots of privacy preserving works. Semi-honest representation necessitates that the entire parties follow protocol but any party may try to find out some data from intermediate results hence our objective is that no knowledge regarding each party data is leaked in this representation.

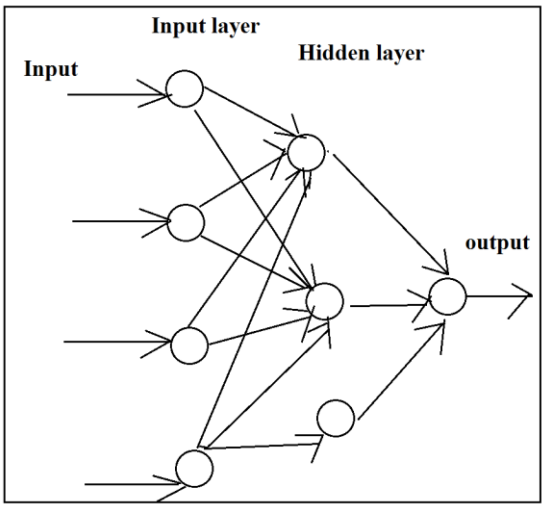

Fig1: overview of Neural Network

3. AN OVERVIEW OF PROPOSED SYSTEM:

Neural Networks was an active research issue for many years. On the other hand, privacy troubles many when training dataset for neural networks is distributed among two parties, which is relatively common these days. There are numerous algorithms of privacy preserving data mining but none of them are used directly within difficulty of privacy preserving neural network learning when training data is randomly divided among two parties. Data providers in support of machine learning are not prepared to train neural network by their information at cost of privacy and though they do take

part in training they may moreover remove some data from their information or else can offer fake information. We present an algorithm of privacy preserving for neural network learning when dataset is randomly partitioned among the two parties so that no party learn anything regarding others party data apart from final weights that are learned by network. When neural networks data is arbitrarily divided among two parties, these parties instruct the network however do not wish to disclose the data to other party. Privacy preserving algorithm in support of neural networks is proficient regarding computational as well as communication overheads [4]. It moreover leaks no information regarding other's party information except final weights that are learned by network training end. Here we consider arbitrary partitioning of data among two parties where there is no order of data separation among two parties and both the parties change weights and include random shares of weights throughout training. These parties use secure two-party computation for computation of random shares of weights between training rounds. There is moreover a general method in cryptography, known as secure multi-party computation that is functional towards privacy preserving problems of neural network learning [5]. Secure multiparty computation solves the entire problems of privacy-preserving working out but, it is extremely costly to be functional when it comes to realistic problems. In some of the situations where neural networks are functional, typically parties hold vast data thus, this common solution is particularly infeasible to our difficulty. It is particularly important that not only data but intermediate weights moreover must not be exposed to other party while intermediate weights hold partial information about data. In the proposed privacy preserving back propagation neural network algorithm after each round of training both parties hold random shares of weights which assures more security against intrusion by other party. It is simply at end of training that both parties recognize actual weights within neural networks [6]. The owner of network allocates random weights towards neural networks in start of training. At end of every round of training, each of the party holds simply a random share of every weight. The back-error propagation stage modifies weights to attain accurate weights within neural network. The algorithm of secure scalar party is used to compute product of two vectors so that at

end of calculation every party holds random share of result with the intention that none of the party is capable to estimate other party's vector. Our proposed algorithm is reasonably secured while intermediate results are randomly shared among the two parties. The experiments performed on actual data explain that quantity of accuracy losses are within the limits.

4. CONCLUSION:

The development of internet has made it simple to collect data from lots of sources. Algorithms of privacy preserving were examined within data mining when data to be mined is distributed between various parties. We present an algorithm of privacy preserving for neural network learning when dataset is randomly partitioned among the two parties so that no party learn anything regarding others party data apart from final weights that are learned by network. Our work suggests privacy preserving algorithm in support of neural networks when data is arbitrarily divided and in this algorithm both parties change weights and include random shares of weights throughout training. Our work considers arbitrary partitioning of data among two parties where there is no order of data separation among two parties and both the parties change weights and includes random shares of weights throughout training. These parties use secure two-party computation for computation of random shares of weights between training rounds. We imagine semi-honest representation which is a principle security representation in lots of privacy preserving works. The proposed system is comparatively proficient regarding computational as well as communication overheads. Our proposed algorithm leaks no information regarding other's party information except final weights that are learned by network training end.

REFERENCES

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

[2] Du, W., Han, Y. S. & Chen, S., (2004). Privacy-preserving multivariate Statistical Analysis :Linear Regression and Classification. Proceedings of the SIAM International Conference on Data Mining.

[3] ElGamal, T., (1985). A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms, IEEE Trans.Information Theory, 31(4). 469-472.

[4] Jagannathan, G. & Wright, R. N. (2005). Privacy-preserving distributed k-means clustering over

arbitrarily partitioned data. In Proc. ACM SIGKDD, 2005, 593-599.

[5] Kantarcioglu, M., & Clifton, C. (2002). Privacy-preserving distributed mining of association rules on horizontally partitioned data. In The ACM SIGMOD Workshop on Research Issues on Data Mining and Knowledge Discovery (DMKD'02).

[6] Kantarcioglu, M., & Vaidya, J. (2003). Privacy preserving naive Bayes classifier for Horizontally partitioned data. In IEEE Workshop on Privacy Preserving Data Mining.