IJRRECS/April 2016/Volume-4/Issue-4/5424-5428 **ISSN 2321-5461**

INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE

AN INTRODUCTION TOWARDS IMPROVED APPROACH FOR NEURAL NETWORK LEARNING

V.Divya[1], Ranjith Kanna[2]

[1]M.Tech Student, Dept of CSE, Ganapathy Engineering College, Warangal, T.S, India

[2]Assistant Professor, Dept of CSE, Ganapathy Engineering College, Warangal, T.S, India

ABSTRACT:

With the discovery of novel technologies in databases or else in any networks, resolving the problems of privacy has turned into extremely important. Since all sorts of data are gathered from lots of sources, field of machine learning is uniformly growing and as a result are the concerns concerning the privacy. There are several algorithms of privacy preserving data mining however none of these are used directly within privacy preserving problem of neural network learning when training data is randomly partitioned among two parties. Here we propose a privacy preserving algorithm in support of back-propagation algorithm of neural network when dataset is randomly partitioned among two parties. We imagine a semi-honest model and our algorithm is relatively secured as intermediate results are arbitrarily shared among the two parties. Our proposed privacy preserving algorithm is the initial approach in support of neural networks when data is randomly partitioned and it is relatively efficient regarding computational as well as communication overheads.

Keywords: Privacy preserving, Data mining, Semi-honest, Neural networks, Training data, Database, Machine learning.

1. INTRODUCTION:

The development World Wide Web has made easy to collect data from numerous sources. Training of neural networks from distributed data is general and when during training of neural network from distributed data, the most important concern is privacy. The most surveys conducted in recent times, from web users suggest that massive percentage of people are worried concerning

their private data release to the exterior world [1]. Data providers in support of machine learning are not eager to guide the neural network by their data at the cost of privacy and although they do take part in training they may moreover eliminate some data from their information or else provides fake information. The datasets that are used in support of neural network training is cooperatively seen as virtual database. Within a distributed data situation this database is partitioned in lot of ways. When some database rows are among one party and other party holds rest of database rows, this indicates horizontal partitioned database and in this case for training of neural network this does not cause an important privacy danger as each of the data holder trains network in turns. When some of the database columns are by one party and other party holds rest of columns, this indicates vertical partitioning of datasets in support of training. In our work we provide an algorithm of privacy preserving for neural network learning when dataset is randomly partitioned among two parties [2][3]. In random partitioning of information among two parties, there is no exact order of how data is divided among two parties. Combined information of two parties is together seen as a database. Our algorithm is extremely secure and leaks no knowledge in relation to data of other party.

2. METHODOLOGY:

Neural Networks was an active research area for many years. Trained neural networks will expect efficient outputs which may be difficult to attain in real world. Training of neural networks from distributed data is common. When training data meant for neural networks is randomly partitioned among two parties, both of the parties want to guide network but simultaneously they do not desire that other party should find out anything concerning its data except final weights learned by network. Hence we provide a privacy preserving back-propagation algorithm of neural network when dataset is randomly partitioned among two parties. Chen and Zhong have proposed an algorithm of privacy preserving in the neural networks when the data of training is vertically partitioned. In the vertical partitioning of datasets, some of the database columns are by one party and other party holds rest of columns. Chen and Zhong algorithm is resourceful and provides tough privacy guarantees. There is yet a different category meant for partitioned data.

The privacy preserving problem of neural network learning above randomly partitioned data was not been solved. Algorithms of privacy preserving was moreover been investigated within data mining when data to be mined is distributed between various parties. There are numerous algorithms of privacy preserving data mining but none of these are used directly within privacy preserving problem of neural network learning when training data is randomly partitioned among two parties. There is moreover a general-purpose method in cryptography, known as secure multi-party computation that is functional towards problems of privacy preserving neural network learning. In our work we provide a privacy preserving algorithm in support of back-propagation algorithm of neural network when dataset is randomly partitioned among two parties so that none of the party is capable to find out anything concerning other's party data apart from the final weights learned by network [4]. To the best of our information our work is the first to suggest privacy preserving algorithm in support of neural networks when data is randomly partitioned. Our algorithm is relatively efficient regarding computational as well as communication overheads. Regarding privacy, our algorithm leaks no data regarding other's party data except for final weights that are learned by network at end of training.

3. AN OVERVIEW OF PROPOSED SYSTEM:

The traditional methods of cryptographic such as secure scalar product procedure make available a safe approach for neural network learning when training dataset is vertically partitioned that is some of database columns are by one party and other party holds rest of columns. Secure multi-party computation is moreover a general-purpose method in cryptography that is functional towards problems of privacy preserving neural network learning. It is extremely significant that when training data meant for neural networks is randomly partitioned among two parties, both of the parties want to guide network but simultaneously they do not desire that other party should find out anything concerning its data except final weights learned by network. Barni et al. has introduced security algorithms for three situations within neural networks such as: When data is being held by means of one party and network parameters are being held by means of

other; when besides weights, other party needs to protect activation function too; when other party needs to protect network topology. Their effort is restricted to the level that simply one party holds data and other holds parameters of the network. We suggest an algorithm where both parties alter the weights and hold arbitrary shares of weights throughout training. Our algorithm is relatively secured as intermediate results are arbitrarily shared among the two parties. In arbitrary partitioning of information among two parties, there is no exact order of how data is divided among two parties. Combined information of two parties is together seen as a database [5]. We imagine a semi-honest model which is a standard security representation in lots of privacy preserving works. Semi-honest representation requires that the entire parties follow procedure but any of the party may attempt to learn some data from the results of intermediate. Hence our intention is that no information with reference to each party's data is leaked within this representation and provide an algorithm in support of algorithm of neural network when dataset is randomly partitioned among two parties so that none of the party is capable to find out anything concerning other's party data apart from the final weights learned by network. ElGamal Encryption method as well as homomorphic property of system is employed within our algorithm. Homomorpic property describes a property of assured algorithms of encryption in which particular algebraic operations are performed above plaintext by means of performing operations on encryption messages devoid of actually decrypting them. In the proposed algorithm subsequent to each of the training rounds both of the parties simply hold random shares of weights and this assurances additional security along with privacy against disturbances by other party [6]. It is only at end of training that both of the parties recognize actual weights within neural networks. The owner of network allocates random weights towards neural networks within beginning of training.

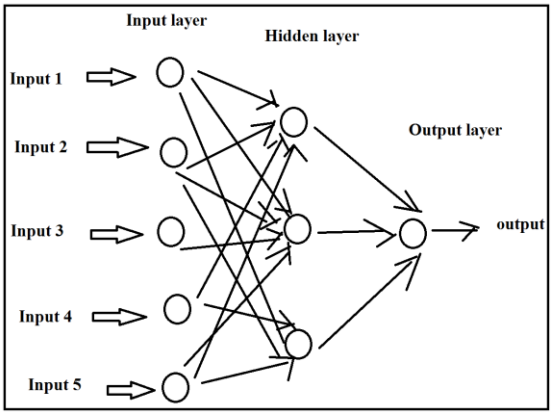

Fig1: An overview of neural networks

4. CONCLUSION:

The expertise of Neural Networks was been an active area of research for so many years. On the other hand, privacy bothers when training of dataset for neural networks is distributed among two parties, which is reasonably general these days. The problem of privacy preserving of neural network learning above randomly partitioned data was not been solved in the earlier works hence we propose a privacy preserving algorithm in support of back-propagation algorithm of neural network when dataset is randomly partitioned among two parties. Here the aim is that none of the party is capable to find out anything concerning other's party data apart from the final weights learned by network. This approach is the initial privacy preserving algorithm in support of neural networks when data is randomly partitioned. It is comparatively efficient regarding computational as well as communication overheads. And moreover concerning privacy, proposed approach leaks no data regarding other's party data except for final weights that are learned by network at end of training.

REFERENCES

[1] 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.

[2] Chang, Y. C., & Lu. C. J. (2001). Oblivious polynomial evaluation and oblivious neural learning, In Proceedings of Asiacrypt, 369-384.

[3] Cranor, L. F., Reagle. J., & Ackerman. M. S. (1999). Beyond concern: Understanding net Users attitudes about online privacy. Technical report TR 99.4.3, AT&T Labs-Research, Available from http://www.research.att.com/library/trs/TRs/99/99.4/99.4.3/report.htm.

[4] Lorrie faith cranor, editor. (1999). Special Issue on Internet Private. Comm.ACM. 42(2).

[5] (2001). Standard for privacy of individually identifiable health information. Federal Register, 66(40).

[6] Goldreich, O.,Micali, S., & Wigderson, A. (1987). How to play ANY mental game, In Proceedings of Annual ACM Conference on Theory of Computing, 218-229.