https://doi.org/10.26438/ijcse/v6si1.3236

IJCSE International Journal of Computer Sciences and Engineering Open Access

Research Paper Volume-6, Special Issue-1, Feb 2018 E-ISSN: 2347-2693

An Encrypted Neural Network Learning to Build Safe Trained Model

S. S. Sayyad[1], D. B. Kulkarni[2]

[1*]Department of Computer Science and Engineering, Annasaheb Dange College of Engineering and Technology Ashta,
[2] Department of Information Technology, Walchand College of Engineering, Sangli,

[*]*Corresponding Author: suhelsayyad2006@gmail.com, Tel.: +91-9881088928*

Available online at: www.ijcseonline.org

Abstract— Neural network learning is a technique that is used to solve problems of classification, prediction, clustering, modelling based on variety of data inputs in the form of structured, semi-structured and unstructured data. Learning accuracy is considered as key performance index in these neural network based learning algorithms. Many organization that involves huge amount of data would want to outsource it to cloud for artificial intelligence based services. Various organization who wish to train neural network model on their complex and huge data usually outsource the learning model on cloud. Outsourcing of learning model on cloud creates security concerns for input data and the learned model. In this paper, we propose a practical system that will train a neural network model that is encrypted during training process. The training is performed on the unencrypted data. The output of the system is a neural network model that possesses two properties. First, neural network model is protected from the malicious users, hence allows the users to train the model in insecure environments at no cost of risk. Second, the neural network model can make only encrypted predictions. We make use of homomorphic encryption techniques to fulfill the objectives and test our results on sentiment analysis dataset.

Keywords—Homomorphic encryption, neural network

I. INTRODUCTION

Neural Network is a mathematical model that is used for solving various kinds of classification and clustering problems. For example, text recognition, speech recognition [19, 20]. A neural network model makes predictions based on the inputs. This model performs this task by trial and error strategy. It begins the process by making a prediction which is random by large at the beginning, later it corrects the error signals received by large and relearns the model till it improves the accuracy to a desired threshold.

In order to train a neural network model in an insecure environment, one must apply encryption mechanism. Homomorphic encryption is a type of encryption mechanism that allows modifying of encrypted information in particular ways without reading the original information. For example, homomorphic encryption can perform addition and multiplication operations on encrypted values without actually decrypting the original data.

II. RELATED WORK

Neural network learning is a kind of machine learning technique which models higher level of abstraction in the data elements. For learning, the network uses multiple processing layers each with multiple non-linear transformations. Neural network learning algorithms, architecture and end user application are mentioned in [17, 18]. Neural network learning algorithms has provided good results for problems on Speech Recognition [19, 20, 21], Image Recognition [22, 23] and Face Detection [24]. Our proposed work is inspired by various advancements in parallelization of deep learning on CPU/GPU based frameworks as well as various techniques for privacy preserving neural network learning.

There are techniques proposed based on secured multiparty computation in which collaborative machine learning can be performed with 2 party, multi-party scenarios. This Secure Multiparty Computation approach has been implemented with decision tree algorithms [25], association rule mining [26], regression based algorithms [27] and KMeans Clustering [28].

Several privacy preserving BPN network learning schemes [3] [5] [9] [10] [11] have been proposed in the past. Jiawei Yuan and Shucheng Yu in [2] propose a technique for Privacy Preserving Back Propagation Algorithm on a cloud environment. The work is concentrated towards providing a solution to a neural network learning problem in which data is arbitrarily partitioned in horizontal and vertical datasets. Schlitter in [3] proposed a privacy preserving back propagation neural network learning scheme. This scheme can be used to provide learning between two or more parties in which the data is horizontally partitioned amongst the participating parties. This technique fails to protect the intermediate results of the learning process. This intermediate results may also contain sensitive information. Chen and Zhong in [5] proposed a privacy preserving back propagation neural network learning for two party problem.

© 2018, IJCSE All Rights Reserved

This learning mechanism can be used to work with vertically partitioned dataset. This technique also provides security to intermediate results. Several mechanisms are working in improving the data security in public domain with help of perturbation techniques. Mohammad Kadampur in [6] has addressed the issue of applying these perturbation techniques to decision tree classifiers in data mining problems. Nathan Dowlin, Ran Gilad-Bachrach, Kim Laine et.al. in [15] proposed Crypto Nets. It is a method that allows the users to send their private data in an encrypted form onto the cloud. The cloud performs all the learning algorithm and returns the result back to the user. The cloud service provider does not learn anything about the input data as it does not have key for the same. The encryption done on the input data ensures that the data remains confidential. Ryan Hayward, Chia-Chu Chiang in [16] built a private cloud that supports parallel processing for homomorphic encryption. They demonstrated it with help of client server model based to evaluate cloud computing of Gentry's encryption algorithm. Yong Liu, Yeming Xiao, Li Wang, Jielin Pan, Yonghong Yan in [7] proposed back propagation neural network learning model for speech recognition. The technique used graphics processing units for parallel reduction in learning process. The technique used asynchronous communication between the CPU and GPU for parallel reduction.

Erich Schikuta and Erwin Mann in [4] presents the N2Sky framework. This framework utilises the sky computing mechanism that provides neural network learning as a service in cloud. The mechanism uses virtualisation to enable learning to be performed on cloud as a service. Mahmoud Barhamgi, Arosha K. Bandara, and Yijun Yu in [12] present various current trends on the security used in Cloud Computing paradigm. It describes the pros and cons of Fully Homomorphic, Partial Homomorphic techniques that are currently used. It also discuss about the Intention Hiding techniques which can be thought of as an alternative solutions to these problems on cloud computing. Majid Bashir Malik in [13] describes privacy preserving approach on data mining algorithms with help of soft computing in terms of fuzzification. The technique proposed ensures the confidentiality of the participating elements and does not make any impact on end result of learning. Reza Shokri in [14] presents a practical system that allows multiple parties associated in learning process to train a neural network model without compromising the security issues of the data inputs. This technique exploits the asynchronous and parallel behaviour of the neural network learning in modern day stochastic based learning models. The technique allows every participating party to independently train on their fragment of data in parallel and share the small sets of their trained model during the training process.

Unlike previous proposed algorithms, our approach helps one to train neural network model in an insecure environment. The data passed to the model is in an unencrypted form. But the predictions made by the model will be encrypted one.

III. METHODOLOGY

Neural networks and homomorphic encryption are often brought together to deal with the problems of data privacy. Homomorphic encryption allows user to encrypt the data and turn it into unreadable form but still maintains its statistical structure. This has made possible to implement systems like CryptoNets [15]. However, our work focuses on opposite concept of the problem. We work on encryption of the neural network and training it on decrypted data.

A. Neural Network Model

A neural network model can be broken down in smaller operations that are repeated again and again. A neural network model can be built by using operations like Addition, Multiplication, Division, Subtraction, and Sigmoid.

For encrypting the neural network model, it is really important to consider above set of operations. Addition and multiplication operations are supported by homomorphic encryption techniques. On the other hand, division and subtraction can be obtained by 1/ multiplication and a negated addition. For sigmoid we need to provide certain approximation. A Taylor series permits to compute a complex nonlinear function using an infinite series of additions, multiplications, divisions and subtraction. Exponents can be simulated as repeated multiplications.

B. Homomorphic encryption

Homomorphic encryption is a new trend in information security which was much accepted after Gentry proposed his first fully homomorphic encryption. There are some drawbacks with fully homomorphic encryption schemes that they are not practically feasible. They are computationally very expensive. Hence less flexible but much faster on operations, somewhat homomorphic encryption schemes are practically feasible ones. There are many choices of homomorphic encryption schemes that can be used

1. Efficient Homomorphic Encryption on Integer Vectors
2. YASHE- Yet Another Somewhat Homomorphic Encryption
3. FV- Somewhat practically fully homomorphic encryption
4. Fully homomorphic encryption with bootstrapping.

In our work, we are implementing efficient homomorphic encryption on integer vector [25]. This technique is less advanced or less secured as compared to other mentioned above. But our idea presented is so generic that any of the techniques mentioned above i.e. homomorphic encryption over addition and multiplication of integers or floating point numbers can be supported.

i. Plaintext: This is unencrypted data. In our work, this will be representing numbers in neural network model.
ii. Cipher text: This is encrypted data. We are applying math operation on plaintext in order to obtain cipher text.

© 2018, IJCSE All Rights Reserved

iii. Public key: This is a random key. It allows encryption of the data. It is permissible that this key is shared in public domain as it is used only for sake of encryption purpose.
iv. Private Key: This is random key. It allows decrypting the data that was encrypted using the public key. It is not permissible to share this key with the people in public domain.

Below mentioned are notation that are used often in the mathematical formulation of our implementation

TABLE I
NOTATIONS IN HOMOMORPHIC ENCRYPTION

Symbol	MEANING
S	Matrix representing secret key/ private key.
M	Public key.
c	Cypher text. Encrypted data matrix
x	Plain text message.
w	Single weighted scalar variable used to re-weight the plain text message x. Used to tune signal/ noise ratio.
E or e	Refers to random noise.

Capital letter symbols signifies matrix, lower letters signifies vectors and italic corresponds to scalars.

Let x be the integer vector that is to be encrypted. Length of this vector is m. Size of alphabet is p. Let c be the cipher text of message x. The length n > m and the alphabet size q >> p. The secret key S is such a key that satisfies the below equation

$$Sc = qk + wx + e \quad (1)$$

for some integer vector k and noise vector e.

The objective of encryption scheme is to find a cipher text c that satisfies above equation for k and noise vector e. As per above equation, decryption of cipher text c based on S is obtained by computing below

$$x = \left\lceil \frac{Sc}{w} \right\rfloor \quad (2)$$

where we try to compute nearest integer value. Homomorphic operations are mentioned below addition operation, weighted inner product and linear transformation.

Further, we provide key switching which allows to change pair of secret key and cipher text to another chosen pair of secret key and cipher text that fulfils encryption of original plain text.

Consider the plain text x which is currently encrypted as c by using a secret key value S and we want to find a new cipher text c' with a new secret key pair S' that satisfies below equation

$$S'c' = Sc \quad (3)$$

In order to achieve above representation we follow two steps. First, we represent the cipher text in bit representation form as below

$$c^* = [\, b_{1,\ldots,}^T b_n^T \,]\, T \quad (4)$$

Next we obtain the new S* matrix from original S matrix as below

$$B_{ij} = [2^{l-1} S_{ij}, \ldots, 2S_{ij}, S_{ij}] \quad (5)$$

For example,

$$S = \begin{bmatrix} 1 & 2 \\ 5 & 4 \end{bmatrix}$$

Will provide

$$S^* = \begin{bmatrix} 4 & 2 & 1 & 8 & 4 & 2 \\ 20 & 10 & 5 & 16 & 8 & 4 \end{bmatrix}$$

That satisfies

$$S^*\, c^* = Sc \quad (6)$$

Second we construct a key switch matrix M that satisfies

$$S'M = S^* + E \quad (7)$$

We have limited our implementation of obtaining new secret key values in the form of S'= [I, T], where identity matrix I is concatenated with some matrix T. Hence we get matrix M as below

$$M = \begin{bmatrix} S^* - TA + E \\ A \end{bmatrix} \quad (8)$$

Further we define

$$c' = M\, c^* \quad (9)$$

And we can clearly observe that

$$S'c' = S^*c^* + Ec^* \quad (10)$$

Based on the above encryption and decryption strategies we expand further operations. Neural network is collection of series of operations.

Vector Matrix Multiplication: M Matrix that converts one key to another key is a way to perform linear transform.

Inner Dot Product: It can also be another form of above linear transform.

Sigmoid: As we can perform vector matrix multiplication, we can compute arbitrary polynomials provided enough number of multiplication operations. We can use Taylor series operation to compute an approximate sigmoid.

Element wise matrix multiplication: This is an inefficient operations. We need to perform series of inner dot products.

Outer Product: We can obtain this by masking and inner products.

IV. RESULTS AND DISCUSSION

Our experimentation is performed on using certain methods and framework viz., NumPy, Pandas, Jupyter Notebook, Bags of Words and Word2vec. We are performing sentiment classification, positive and negative in movie reviews. Total number of review instances available are 25000. The dataset comprises of two files viz., reviews that contains reviews of 25000 movies and labels file which indicates target labels for respective movie reviews.

© 2018, IJCSE All Rights Reserved

We create a vocabulary list across all the reviews. For every term in vocabulary list we find positive to negative ratio of each term in vocabulary list. This helps us determine most frequently seen terms in a positive review. Table II indicates various learning parameters set for the training. Scaling factor is required in our experimentation to convert floating point operands to integers. Homomorphic scheme used in our implementation supports only integer vectors.

Table II. Non Privacy and Privacy Preserving Training Analysis

Dataset	Total number of instances	Learning Rate	Scaling Factor
Sentiment Analysis	25000	0.001	1000

We have performed experimentation on Intel Core i3 3.10 GHz with 2 GB RAM. Sentiment analysis was carried out for non-privacy preserving (Non PP) model and privacy preserving (PP) model. Accuracy of training was measured. Table III indicates training accuracy of sentiment analysis.

Table III. Non Privacy and Privacy Preserving Training Analysis

Dataset	Non PP		PP	
	Correct Trained	Accuracy (%)	Correct Trained	Accuracy (%)
Sentiment Analysis	20523	82.0	18799	75.1

Accuracy for training was measures as below for encrypted neural network learning and simple plain text learning.
Our work supports following operations using homomorphic encryption over encrypted domain namely addition, weighted inner products and linear transformation.

A. Addition

Suppose, x1 and x2 are plain text and their corresponding cipher text are c1 and c2. We can observe that

$$S\,(c_1 + c_2) = w(x_1 + x_2) + (e_1 + e_2)$$

In order to perform addition of two plain text in encrypted domain, we perform addition of their respective cipher text provided that both the plain text are encrypted with same secret key. Hence new cipher text can be obtained as

$$c' = c_1 + c_2$$

While the secret key remains the same.

B. Linear Transformation

Suppose for a given plaintext x and its respective cipher text c with help of secret key value S, we can obtain a linear transformation Gx by

$$(GS)c = xGx + Ge$$

C. Weighted Inner Product

We consider example of matrix vector product here. Consider vec (M) be a vector representation of matrix M. Then we have following implication. For any vector x, y and given matrix M of related dimension

$$x^T My = vec(M)^T\ vec\ (xy^T)$$

The above expression can be justified with help of below mentioned proof.

$$\begin{aligned} vec(M)^T\ vec\ (xy^T) &= \sum_i \sum_j M_{ij} x_i y_j \\ &= \sum_j \left(\sum_i x_i\, M_i \right) . y_j \\ &= \sum_j (x^T M)_j\ y_j \\ &= x^T My \end{aligned}$$

V. CONCLUSION and Future Scope

Learning based on encrypted models is a unique direction in cloud based neural network learning. Learning models deployed on cloud raise security concerns about the model to be trained. Our scheme provides a unique solution for training on the encrypted model using homomorphic encryption. Our work demonstrates that complex operations involved in neural network learning can be easily broken to smaller operation that are supported by homomorphic encryption. We have demonstrated learning results for encrypted models using efficient integer vector homomorphic encryption. This work can be extended by using schemes like YASHE for supporting floating point operations over the training data. This will remove the dependency with the scaling factor in our implementation. Our work leads to many potential applications like decentralised artificial intelligence, controlled super intelligence etc.

REFERENCES

[1] S. Chow, Y. He, and et al. Spice - simple privacy-preserving identity-management for cloud environment. In ACNS 2012, volume 7341 of Lecture Notes in Computer Science. Springer, 2012.

[2] Privacy Preserving Back-Propagation Neural Network Learning Made Practical with Cloud Computing. IEEE Transactions on Parallel and Distributed Systems, Vol. 25, No. 1, January 2014.

[3] N. Schlitter, A Protocol for Privacy Preserving Neural Network Learning on Horizontal Partitioned Data, Proc. Privacy Statistics in Databases (PSD 08), Sept. 2008

[4] Erich Schikuta and Erwin Mann, N2Sky - Neural Networks as Services in the Clouds. arXiv:1401.2468v1 [cs.NE] 10 Jan 2014.

[5] T. Chen and S. Zhong,Privacy-Preserving Backpropagation Neural Network Learning, IEEE Trans. Neural Network, vol. 20, no. 10, pp. 1554-1564, Oct. 2009.

[6] Mohammad Ali Kadampur, Somayajulu D.V.L.N. A Noise Addition Scheme in Decision Tree for Privacy Preserving Data Mining, Journal of Computing, Volumen 2, Issue 1, January 2010, ISSN 2151-9617

[7] Yong Liu, Yeming Xiao, Li Wang, Jielin Pan, Yonghong Yan. Parallel Implementation of Neural Networks Training on Graphic Processing Unit, 2012 5th International Conference on BioMedical Engineering and Informatics (BMEI 2012)

[8] Pelin Angin, Bharat Bhargava, Rohit Ranchal, Noopur Singh. An Entity-centric Approach for Privacy and Identity Management in Cloud Computing, 2010 29th IEEE International Symposium on Reliable Distributed Systems.

© 2018, IJCSE All Rights Reserved

[9] Scretan J, Georgiopoulos, M. A privacy preserving probabilistic neural network for horizontally partitioned databases. International Joint Conference on Neural Networks. Aug 2007.

[10] Barni M, Failla P, Sadeghi A. Privacy Preserving ECG Classification with branching programs and neural networks.IEEE Transaction. Information Forensics and Security. Volume 6, Issue 2, June 2011.

[11] Samet S. Privacy Preserving protocols for perceptron learning algorithm in neural networks. IEEE Conference on Intelligent Systems, Sept 2008.

[12] Mahmoud Barhamgi, Arosha K. Bandara, and Yijun Yu, Protecting Privacy in the Cloud: Current Practices, Future Directions, Computer IEEE Society February 2016.

[13] Majid Bashir Malik, A model for Privacy Preserving in Data Mining using Soft Computing Techniques. March 2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom).

[14] Reza Shokri, Privacy-Preserving Deep Learning,, 2015 53rd Annual Allerton Conference on Communication, Control, and Computing (Allerton) Oct 2015.

[15] Nathan Dowlin, Ran Gilad-Bachrach, Kim Laine, Kristin Lauter, Michael Naehrig and John Wernsing, CryptoNets: Applying Neural Networks to Encrypted Data with High Throughput and Accuracy 29 December 2015

[16] Ryan Hayward , Chia-Chu Chiang, Parallelizing fully homomorphic encryption for a cloud environment. Journal of Applied Research and Technology 13 (2015) 245-252

[17] Bengio. Learning deep architectures for AI. Foundations and trends in machine learning, 2(1):1– 127, 2009.

[18] L. Deng. A tutorial survey of architectures, algorithms, and applications for deep learning. APSIPA Trans. Signal and Information Processing, 3, 2014.

[19] A. Graves, A.-R. Mohamed, and G. Hinton. Speech recognition with deep recurrent neural networks. In ICASSP , 2013.

[20] Hannun, C. Case, J. Casper, B. Catanzaro, G. Diamos, E. Elsen, R. Prenger, S. Satheesh, S. Sengupta, A. Coates, et al. Deepspeech: Scaling up end-to-end speech recognition. arXiv:1412.5567 , 2014.

[21] G. Hinton, L. Deng, D. Yu, G. Dahl, A.-r. Mohamed, N. Jaitly, A. Senior, V. Vanhoucke, P. Nguyen, T. Sainath, et al. Deep neural networks for acoustic modeling in speech recognition: The shared views of four research groups. Signal Processing Magazine , 29(6):82–97, 2012.

[22] A. Krizhevsky, I. Sutskever, and G. Hinton. Imagenet classification with deep convolutional neural networks. In NIPS , 2012.

[23] P. Simard, D. Steinkraus, and J. Platt. Best practices for convolutional neural networks applied to visual document analysis. In Document Analysis and Recognition , 2013.

[24] Y. Taigman, M. Yang, M. Ranzato, and L. Wolf. Deepface: Closing the gap to human-level performance in face verification. In CVPR , 2014.

[25] Angel Yu, Wai Lok Lai, James Pay or Efficient Integer Vector Homomorphic Encryption, May 2015.

Authors Profile

Mr. S S Sayyad is a research scholar at Walchand College of Engineering, Sangli. He has completed his M.Tech in Computer Science and Engineering from Walchand College of Engineering, Sangli in 2012 and B.E in Computer Science and Engineering from Karmaveer Bhaurao Patil College of Engineering, Satara in 2007. His areas of interest are High Performance Computing, Cloud Computing. He is currently working as Assistant Professor at Annasaheb Dange College of Engineering and Technology Ashta for last 8 years. He also has 2 years of industrial experience as Software Engineer at Zensar Technologies, Pune.

Dr. D B Kulkarni received the doctorate degree in Computer Science and Engineering from Shivaji University, Kolhapur in the year 2005. Currently he is a professor in Information Technology Department of Walchand college of Engineering, where he teaches many courses in the area of Computer Science. During his professional life, he has been involved in several R&D projects funded by AICTE, DRDO and UGC. Recently he received Early Adopter award of National Science Foundation's (NSF) of Technical Committee on Parallel Processing (TCPP) of US$1500 for framing and adapting curriculum on “Parallel Computing” in UG and PG curriculum in the institute. He was Visiting Professor in institute of Computer Technology (ICT) of Vienna University of Technology, Austria, in 2010. He is coauthor of tens of scientific papers published in international journals and conference proceedings. His research interests include the area of High Performance computing and Computer Network.

© 2018, IJCSE All Rights Reserved