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 5, May 2017

# Privacy Preserving Back-Propagation Neural Network with Cloud

**Kalpana Vyavahare [1], Aniket Khobragade[2], Pratiksha Wankhade[3], Atthar Mansuri[4], Sampada Kulkarni[5]**

Student, Computer Engineering, D.Y Patil College of Engineering, Ambi, Pune, India[1,2,3,4]

Professor, Computer Engineering, D.Y Patil College of Engineering, Ambi, Pune, India[5]

**Abstract**: To improve the accuracy of learning result, in observe multiple parties might collaborate through conducting joint Back propagation neural network learning on the union of their several knowledge sets. throughout this method no party needs to disclose her/his non-public knowledge to others. Existing schemes supporting this type of cooperative learning are either restricted within the means of information partition or simply take into account 2 parties. There lacks an answer that enables two or a lot of parties, every with an at random partitioned off information set, to collaboratively conduct the training. This paper solves this open drawback by utilizing the ability of cloud computing. In our planned theme, every party encrypts his/her non-public knowledge regionally and uploads the ciphertexts into the cloud. By firmly offloading the high-ticket operations to the cloud, we tend to keep the computation and communication prices on every party nominal and freelance to the amount of participants. To support versatile operations over ciphertexts, we tend to adopt and tailor the BGN 'doubly homomorphic' coding algorithmic rule for the multi-party setting. Numerical analysis and experiments on goods cloud show that our theme is secure, economical and correct.

**Keywords**: Privacy reserving, Neural Network, Back-Propagation, Cloud computing, Computation Outsource.

## I. INTRODUCTION

Neural Network consists of extremely interconnected process component referred to as nerve cell. this is often having restricted number of input and output. Coming up with or programmed this technique for learn the acknowledge pattern. Learning may be supervised or unsupervised. In supervised learning there's a master for monitor the network learning activity wherever as in unsupervised learning there's no master for observation the training. Back-propagation is one in all the strategies for learning the neural networks and has been wide employed in varied applications. the training accuracy is principally tormented by knowledge used for learning. Rather than learning with restricted dataset cooperative learning improve the training result.

In this cooperative learning the taking part parties do learning not solely on their own knowledge sets, conjointly on others' knowledge sets. With the recent new computing surroundings like Cloud Computing, so as to supply sensible solutions for privacy conserving back-propagation neural (BPN) network learning, there square measure chiefly 3 challenges:

1) Give protection to every participant's personal dataset and intermediate results created throughout the BPN network learning method. It needs secure computation of varied operations.

2) make sure the utility of the projected resolution; the computation/communication value introduced to every participant shall be economical. so as to support an outsized vary of cooperative learning, the projected resolution shall take into account system quantifiability

3) During this cooperative leaning coaching dataset closely-held by totally different parties however divided in at random ways that.

## II. LITERATURE REVIEW

**1. "A review of scalable data sharing techniques for secure cloud storage:"**
**Aditi Tripathi, Mayank Deep Khare, Pradeep Kumar Singh**

Cloud computing may be a technology that provides a shared pool of configurable IT resources like network, package and information. Cloud Computing provides the power of centralized knowledge storage, user will access their knowledge on-line. Cloud storage is extremely standard currently a days. Knowledge that is hold on on clouds ought to be secure from adversaries. In cloud storage knowledge sharing is a vital practicality. Knowledge transfer ought to be done firmly and expeditiously with others in cloud computing. During this paper we tend to review totally different ascendable knowledge sharing techniques in cloud storage. To reduce the expense of managing and storing secret keys

DOI10.17148/IJARCCE.2017.6558

for general cryptologic use is aim of cryptologic key assignment schemes. For supporting versatile hierarchy in decipherment power delegation, a encoding theme is depicted that is largely planned for in short transmittal sizable amount of decipherment keys in broadcast situation. to guard information privacy may be a central question for cloud storage. we tend to illustrate new public-key encoding theme, that produces constant-size cipher texts like economical delegation decoding rights for any set of cipher texts square measure attainable.

**2 .“ Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage:”**
**Cheng-Kang Chu , Sherman S.M. Chow, Wen-Guey Tzeng**
Data sharing is a vital practicality in cloud storage. During this paper, we have a tendency to show a way to firmly, expeditiously, and flexibly share information with others in cloud storage. we have a tendency to describe new public-key cryptosystems that turn out constant-size ciphertexts specified economical delegation of decoding rights for any set of ciphertexts are potential. The novelty is that one will mixture any set of secret keys and create them as compact as one key, however encompassing the facility of all the keys being aggregate. This compact mixture key are often handily sent to others or be keep during a} positive identification with very restricted secure storage. we offer formal security analysis of our schemes within the commonplace model. we have a tendency to conjointly describe different application of our schemes. Above all, our schemes offer the primary public-key patient-controlled secret writing for versatile hierarchy that was nonetheless to be well-known.

**3. “Linear Function Based Transformation Scheme for Preserving Database Privacy in Cloud Computing:” Min Yoon, Hyeong-il Kim , Miyoung Jang**
Because a lot of interest in spacial information in cloud computing has been attracted, studies on protective location information privacy in cloud computing are actively done. However, since the present spacial transformation schemes square measure weak to proximity attack, they can not preserve the privacy of users who get pleasure from location-based services from the cloud computing. Therefore, a metamorphosis theme for providing a secure service to users is needed. So, we, during this paper, propose a brand new transformation theme supported a line even transformation (LST). The planned theme performs each LST-based information distribution and error injection transformation for preventing proximity attack effectively. Finally, we have a tendency to show from our performance associatealysis that the planned theme greatly reduces the success rate of the proximity attack whereas activity the spacial transformation in an economical manner.

**4. “Data integrity and security in cloud environment using AES algorithm:”**
B. Thiyagarajan ,R. Kamalakannan
Cloud computing is that the recent emerging technology of IT trade. Virtually each enterprise application is moved to cloud that raised the priority regarding the integrity and privacy of information of consumer also as enterprise officers. the most goal of cloud competitory is a way to secure, defend the information and method. AES formula is of the out sourced information in cloud surroundings the "effective automatic information reading protocol" and multi server information compression formula with efficiency check.

**5 .Review Techniques of Data Privacy in Cloud Using Back Propagation Neural Network:**
**D. J. Bonde1, Shaikh Akib2, Pokharkar Shubhangi3, Auti Surbhi4, Shelke Satish**
Back Propagation is that the theme for neural network learning. This learning accuracy gained by cooperative learning. In existing system support this sort of learning on restricted dataset and between 2 parties. It cannot defend intermediate result. In our planned system multiple parties perform cooperative learning on haphazardly divided knowledge exploitation cloud computing. within which for privacy preservation every party send plain text to the cloud and cloud encode that text. during this means minimizing the computation and communication price. To support the assorted operations over cloud we have a tendency to are exploitation the various algorithmic rule. during this means cloud show our learning theme is secure.

## III.PROPOSED SYSTEM

Several privacy conserving BPN network learning schemes are planned recently. Schlitter[19] introduces a privacy conserving BPN network learning theme that allows 2 or additional parties to conjointly perform BPN network learning while not revealing their individual personal knowledge sets. however the solution is planned just for horizontal partitioned off knowledge. Moreover, this theme cannot defend the intermediate results, which can conjointly contain sensitive knowledge, throughout the training method. Chen et. al.[6] proposes a privacy conserving BPN network learning algorithmic program for 2 party situations. This scheme provides sturdy protection for knowledge sets as well as intermediate results. However, it simply supports vertically partitioned off knowledge. to beat this limitation, Bansal et. al.[4] increased this theme and planned a solution for haphazardly partitioned off knowledge. notwithstanding, this increased theme, rather like [6], was proposed for the two-party state of affairs. Directly extending them to the multi-party setting can introduce a computation/ communication complexness quadratic within the range of participants.

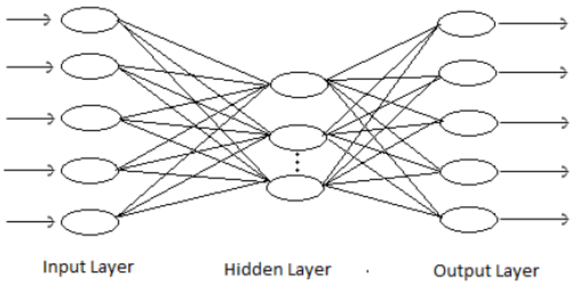


Figure 1: BPN Network

In planned system design trustworthy Authority (TA) is answerable for user registration and authentication. encoding are going to be distributed exploitation uneven key encoding rule. consumer sends plaintext over Cloud. Encrypted information and key keep in information. once user desires to retrieves its original information key of that specific user match with key that is keep at the server aspect information. That key matching method done by neural network. Cloud then rewrite that information and send to consumer.

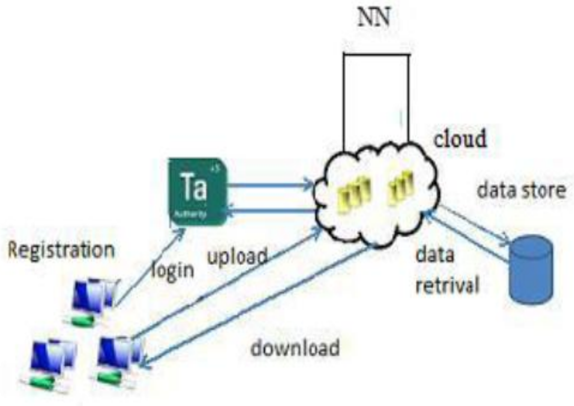


Fig.2 Architecture view of Proposed System

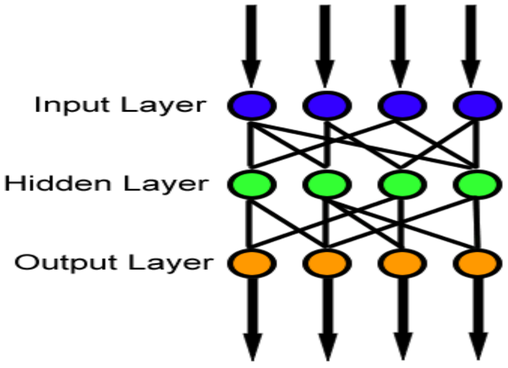
Different functions are carried by this technique are user registration, login, file transfer, cryptography and key generation, file transfer etc.

i. User Registration on cloud is meted out by sure Authority. Ta registers the user data on cloud and stores user data on cloud knowledge store.
ii. once user desires to perform any operation he must login 1st. The login is attested by tantalum.
iii. when login authentication once user desires to transfer any file he requests to cloud to transfer a such file then cloud encrypts that file.
iv. Encrypted file associated generated key's hold on in knowledge store conjointly it sends a key to user as an acknowledgement that is any used for downloading a file.
v. once user desires to transfer his file, once more he must specify a file name and key that is obtained in response whereas uploading a file. Neural network verifies a key and corresponding get in information if it's valid cloud once more decrypts that file with the assistance of key and sends back a decrypted file i.e. original file.

## IV. IMPLEMENTATION

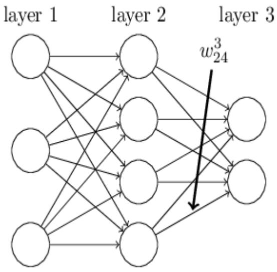
A feedforward neural network is an artificial neural network whereby connections between the units don't type a cycle. As such, it's completely different from repeated neural networks.
The feedforward neural network was the primary and simplest form of artificial neural network devised. during this network, the data moves in mere one direction, forward, from the input nodes, through the hidden nodes (if any) and to the output nodes. There are not any cycles or loops within the network.

DOI10.17148/IJARCCE.2017.6558



The reason, of course, understands. At the center of back propagation is an expression for the partial|derivative|differential coefficient|differential|first derivative} ∂C/∂w∂C/∂wof the price function CC with relevance any weight ww (or bias bb) within the network. The expression tells USA however quickly the price amendments once we change the weights and biases. And whereas the expression is somewhat complicated, it conjointly encompasses a beauty thereto, with every component having a natural, intuitive interpretation. so back propagation is not just a quick algorithmic rule for learning. It really provides USA careful insights into however dynamical the weights and biases changes the behaviour of the network.

Let's begin with a notation that lets consult with weights within the network in Associate in Nursing unambiguous method. We'll use to denote the load for the association from the kth neuron within the (l - one )th layer to the jth nerve cell within the lth layer. So, for instance, the diagram below shows the load on a association from the fourth nerve cell within the second layer to the second neuron within the third layer of a network



$w^l_{jk}$ is the weight from the $k^{\text{th}}$ neuron in the $(l-1)^{\text{th}}$ layer to the $j^{\text{th}}$ neuron in the $l^{\text{th}}$ layer

This notation is cumbersome initially, and it will take some work to master. however with a little effort you will find the notation becomes simple and natural. One quirk of the notation is that the ordering of the j and k indices. you would possibly assume that it makes a lot of sense to use j to discuss with the input somatic cell, and k to the output somatic cell, not the other way around, as is really done.

We use an analogous notation for the network's biases and activations. Explicitly, we have a tendency to use for the bias of the jth somatic cell within the lth layer. and that we use for the activation of the jth somatic cell within the lth layer. the subsequent diagram shows samples of these notations in use:

The four elementary equations behind back propagation:

Back propagation is concerning understanding however dynamical the weights and biases in an exceedingly network changes the price perform. Ultimately, this suggests computing the partial derivatives ∂C/∂wljk and ∂C/∂bjl. however to cipher those, we have a tendency to initial introduce associate degree intermediate amount, δjl, that we have a tendency to decision the error within the jth somatic cell within the lth layer. Backpropagation can provide North American nation a procedure to cipher the error δjl, and so can relate δjl to ∂C/∂wjkl and ∂C/∂bjl.

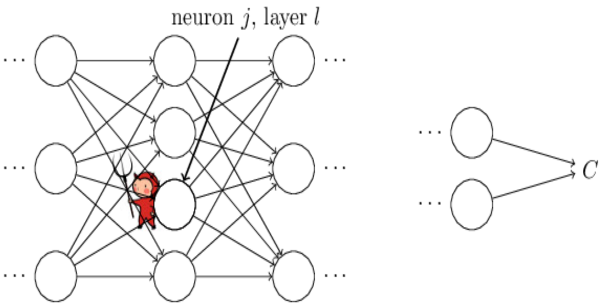
To understand however the error is outlined, imagine there's a demon in our neural network

The demon sits at the jth nerve cell in layer l. because the input to the nerve cell comes in, the demon messes with the neuron's operation. It adds somewhat modification Δzjl to the neuron's weighted input, so rather than outputting σ(zjl), the vegetative cell instead outputs σ(zlj+Δzlj).This change propagates through later layers within the network, finally inflicting the general price to vary by Associate in Nursing quantity ∂C∂zj/Δzjl.

Back propagation relies around four elementary equations. Together, those equations offer us the way of computing each the error δlδl and also the gradient of the value operate.

DOI10.17148/IJARCCE.2017.6558

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



## V. RESULT ANALYSIS

Our planned system has benefits in terms of computation and communication value. because the variety of participant will increase or knowledge size will increase that don't have an effect on the system performance.

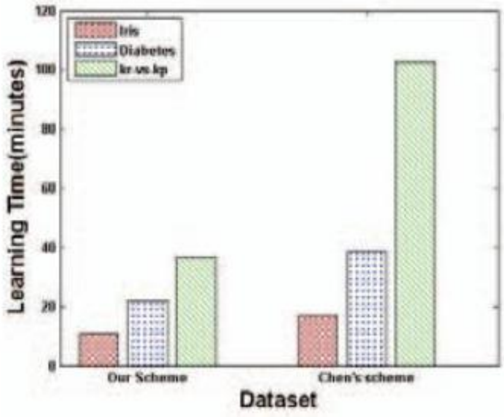


Fig.4 Dataset

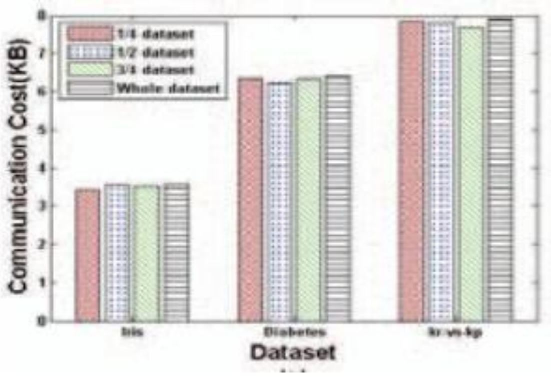
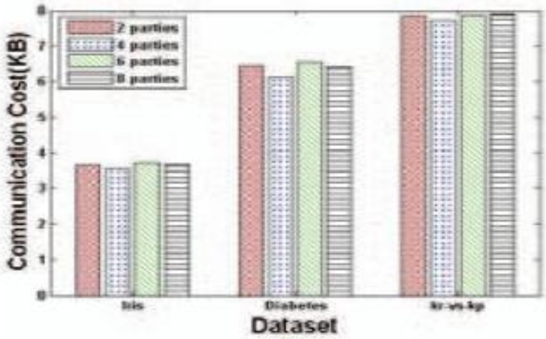


Fig: (a)



Fig; (b)

DOI10.17148/IJARCCE.2017.6558

Learning potency measured in term of learning time. Increased value on every party measured in term of learning time. for 2 party state of affairs compare our learning theme with Chen's theme in term of learning time for various dataset like iris, Diabetes, kr-vs-kp. [1]

When the quantity of parties varies from a pair of to eight, the learning time stays stable in our theme, that is concerning ten.68 minutes, 21.86 minutes and thirty six.69 minutes for Iris, polygenic disorder and kr-vs kp severally. the training time doesn't modification with the quantity of parties as a result of the cloud performs most learning operations in parallel while not learning the personal knowledge. because the variety of party will increase the communication value on every party remains stable throughout the training method as shown in fig. (a)This is as a result of the degree of information for every party to Exchange remains constant because the total variety of parties' changes. [1]
Fig (b) shows that the expansion of dataset size has slight influence on every party's communication value in our theme throughout the cooperative learning method.

## VI. CONCLUSION

We 1st planned secure and sensible multiple-party Back Propagation Neural network learning theme over indiscriminately divided knowledge. In our planned system approach, the parties transfer plaintext to the cloud. The cloud will execute most operations like cryptography, secret writing over that knowledge. Once participant parties need his/her original knowledge once more secret is provided which key matching method allotted by neural network. During this manner protective privacy of every participant's knowledge is achieved. In our sensible approach we tend to are securing the intermediate result. Therefore we tend to minimizing Computation and communication price.

## ACKNOWLEDGMENT

The heading of the Acknowledgment section and additionally the References section shouldn't be numbered. It offers us nice pleasure in presenting the preliminary project report on 'Privacy Preserving Back-Propagation Neural Network with Cloud '. I'd would like to require this opportunity to impart my internal guide for giving me all the help and steering I needed. I am terribly grateful to them for his or her kind support. Their valuable suggestions were terribly helpful. I'm to boot grateful to move of COMPUTER ENGINEERING Department, DYPCOE Ambi, for his indispensable support, suggestion. Within the end our special owing to completely different Person Name for providing varied resources like laboratory with all needed computer code platforms, continuous net association, for Our Project.

## REFERENCES

[1] Privacy Preserving Back-Propagation Neural Network Learning Made Practical with Cloud Computing Jiawei Yuan, Student Member, IEEE, Shucheng Yu, Member, IEEE, 2013

[2] T. Chen and S. Zhong Privacy-preserving back propagation neural network learning. Trans. Neur. Netw., 20(10):1554-1564, Oct. 2009. L. Cun, B. Boser, J. S. Denker, D. Henderson, R. E. Howard, W. Hubbard, and L. D. Jackel. Handwritten digit recognition with a back-propagation network. In Advances in Neural Information Processing Systems, pages 396-404. Morgan Kaufmann, 1990.

[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] Wernik, Yang, Brankov Yourganov and strother, machine learning in medical imaging vol.27 no.4 july 2010 pp 25-38

[5] A fast Nearest Neighbor classier based on self-organizing incremental neural network-Shen Furao, Osamu Hasegawa (2008).

[6] A. Bansal, T. Chen, and S. Zhong. Privacy preserving back propagation neural network learning over arbitrarily partitioned data. Neural Compute. Appl., 20(1):143-150, Feb. 2011.

[7] A. C. Yao. Protocols for secure computations. In Proceedings of the 23rd Annual Symposium on Foundations of Computer Science, SFCS '82, pages 160-164, Washington, DC, USA, 1982.

DOI10.17148/IJARCCE.2017.6558