International Journal of Engineering Research in Electronic and Communication Engineering (IJERECE) Vol 3, Issue 5, May 2016

A Novel Survey on Neural Network Based Cloud Computing Platform for Securing Data

Santosh
School of Electronics and Communication Engineering
Reva University, Bangalore-560064
sjeenagar7@gmail.com

***Abstract*— Current technological advancement of internet or online platform made tremendous changes in the modern human society. Now a days situation has been created in such a way that whatever we want we would like to go for online, it may be shopping, marketing, banking, purchasing of goods, real estate, agricultural, collaborative learning through on line, pharmaceutical industries, medical field etc. When folks think of online activities there is always a feel of insecurity of their transaction, private data, mode of operation, etc. So there is indeed of vital solution which guarantees the security of operation, safety of private data, protectant environment for on line activities. Cloud computing gives the best online environment for various internet based activities. Here we discuss, analyze and understand the cloud computing environment for data security using Back propagation neural networks (BPN).**

***Index Terms*—Back propagation neural networks (BPN), Neural Network (NN), Artificial neural network (ANN).**

I. INTRODUCTION

Neural Network(NN) is framed with an arrangement of inputs and output units which are associated, and every association has a weight connected with it. Neural system requires a long training period. Commonly neural system is basically trained or given a lot of information and standards about information relationship. Neural systems are appropriate for continual esteemed input and output, effective on a wide cluster of true information. The algorithm utilized as a part of neural system are normally parallel which accelerate the calculation process. NN is the set of nodes (hubs) and edges. The edges are connected with a weight and there is an initiation capacity connected with the system that takes weights as inputs and creates the desired output. Back-propagation is one among the vital strategies for learning of the neural systems and has been broadly utilized as a part of different applications. Back spread strategy works in reverse, it computes the mistake between output (expected values) and figured values and prepares neural system until the outcomes are close to expected qualities. The learning exactness is basically influenced by information utilized for learning. Rather than learning with restricted dataset, cooperative learning enhance the learning result. In joint learning more than two users included in learning procedure and they can utilize information of different users, so the protection of private information is imperative here. For joint learning cloud is the best foundation. Cloud is a base which gives assets and administrations over the web. Distributed computing platform provides an expansive huge computation calibre, where the calibre is adjustable in the cloud. By utilizing the cloud which spares the time and application can create and convey quicker. Distributed computing is an innovation which utilizes the internet and focal remote servers to keep up information and applications. Distributed computing permits clients to utilize applications without establishment and access their own records at any PC with web access. This cloud computing technology takes into consideration substantially more effective computation by centralizing information storage, processing and data transfer capacity. A basic sample of distributed computing is Gmail, Yahoo, Email etc.

Generally there are four sorts of distributed computing arrangements: public cloud, private cloud, hybrid cloud and community cloud. In public cloud, the clients get to the cloud by means of interfaces utilizing the web programs. Thus, the client required to pay just for the span of time of services utilization. This will lessen the operation costs. Public cloud are very less safe in contrasted with different cloud models, as all the software and information on this model are more weaker against different assaults .In the private cloud, complete operations of this model are inside of an association's server farms. This model is like the Intranet. The fundamental point of preference is that it is anything but difficult to oversee the security and the upkeep and overhauls are highly controlled. Contrasted with the public cloud where each administrative services and the applications are situated outside the association, in private entity these administrations and applications are accessible at the

association level .The hybrid entity is ablend of not only open cloud but also private cloud. In this entity, a personnel cloud is connected to one or many outside cloud administrations. It empowers the association to address its issue in the private cloud, if some intermittent requirements happen. It approaches the public cloud to get concentrated figuring assets. At long last, the community cloud happens when numerous association together build and distribute the cloud foundation, the necessities and polices.

Challenges*:* To grasp the broad cooperative learning, it is basic to give a solution that permits the participants, who need common trust, to lead neural system adapting mutually without unveiling their individual private information sets. Ideally, the solution might be effective and sufficiently adaptable to strengthen a self-assertive group of participants, each having arbitrarily divided information sets. Hypothetically, secure multiparty calculation (SMC) can be utilized to tackle issues of this type. In any case, to that of a great degree high calculation and correspondence multifaceted nature of SMC, because of the circuit size, for most of the time makes it far away from practical without great variation in the double-party case.

To give real answers for security saving Back-Propagation neural (BPN) system learning, three primary difficulties should be met at the same time: 1) To secure every member's private information set and transitional results created amid the BPN system learning process, it requires privacy calculation of different operations, for instance, the nonlinear sigmoid capacity, addition, and scalar product, which are required by the BPN system calculation;2)Specifically, it should have the capacity to bolster a self-assertive number of participants without presenting huge calculation/correspondence expenses to every user; 3) for joint training, the preparation information sets might be possessed by various clients and partitioned in discretionary routes as opposed to a solitary method for partition.

The paper is arranged as follows. In Section 2, Basic overview BP-based neural network is introduced. The Back propagation Algorithm Various Encryption schemes for securing data are detailed in Section 3. The Various solutions put forth so far are discussed in Section 4. Conclusion is mentioned at final section

II. BASIC OVERVIEW

Cloud computing framework comprises of two primary parts those are associated with each other by means of the Internet: front-end as well as back-end. The front-end is the part that the client can have a look and has on its own system with the necessary applications to associate with cloud computing. The back-end part is nothing but the cloud framework with all collection of information further more administrations for example, programming, servers and information stockpiles. Three distinctive distributed computing models as follows: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). SaaS model provides finalized application to the end-clients by means of the Internet. Accordingly, end-clients dont have to introduce the software as well as related applications in their systems that are adjusted and oversaw by main authority. PaaS gives a working framework, programming dialects and programming improvement by means of the cloud foundation. IaaS, gives the necessary infrastructure as an administration, for example, handling, server farms and system asset. Neural system comprises of three or many layers and every layer has number of functioning units called neurons. It has information layer, resultant layer and concealed layers.

ANN join the info layers with the resultant layers utilizing concealed layers with nonlinear drastic change in functioning and weighted associations. Artificial systems can have diverse number of layers and distinctive number of nodes. The way of the issue and the level of complexity are controlled the number of concealed layers and their respective neurons. The nonlinear change capacities give preference over the estimated functions.

Applications of neural network: Applications of neural network neural system has been generally utilized so far. There are different sorts of algorithms and mechanism taking into account neural system in software engineering territory that were connected to a wide range of angles. As many as there are different variables haphazardly coming and the client needs to decide or illuminate something as per them, neural system would be decent decision because of its self learning and sorting out capacity. Here are a few occurrences.

As appeared in Ref. [8], a fascinating exploration is carried out by substituting variables for example, dampness, titratable sharpness, free unsaturated fats, tyrosine, as well as peroxide esteem into an Artificial Neural Network (ANN) and adding to the model of outspread premise (definite fit) simulated neural system for assessing the time span of usability of burfi put away at 30 degree Celsius; the output estimation of similar kind model will be more valuable, and the outcomes turn out great. Another applicable work is done in Ref. [9] that introduces the capability of Cascade Back propagation calculation dependent ANN models in distinguishing the timeframe of realistic usability of prepared cheddar put away at 30

degree Celsius. The creators quicken using so as to learn in ANNs the Cascade back propagation calculation algorithm (CBA), also the Bayesian regularization calculation was utilized for preparing the system. In Ref. [10], the creators portray another way to deal with breaking down street pictures which frequently contain vehicles and license Plate (LP) from common properties by discovering vertical and flat edges. A calculation in light of fake neural system is utilized for acknowledgment of Korean plate characters in this paper.Ref. [11] Presents an outspread premise capacity manufactured neural system, in which many layer encourage forward system is utilized to manage hydrological information. In RBFANN, spread and focus qualities are the model parameters those are evaluated by inciting the appropriate weight values.

In Ref. [12], the authors are going for the issue of the vulnerability of the calorific estimation of coal; a delicate estimation model towards the calorific estimation of coal is proposed in view of the RBF neural system. Whats more, joined with the considered k-cross approval, the hereditary calculation built a wellness capacity to enhance the RBF system parameters. The BP dependent neural system technique is circulated in Ref. [13] which is proficient for tackling the activity stream issue - a complex non-straight forecast of an expansive scale framework. This is successful since NN Model has versatile and auto-learning capacity. Additionally Ref. [14] demonstrates arrangement of various sorts of targets (vehicles) in the smart Transport Framework. Regulated ANN is utilized as the delicate computing tool for characterization, here targets are ordered on the premise of returned vitality to the Radar then again Radar Cross Section (RCS) estimates taken at various perspective edges. In Ref. [15], the authors examine and decide the elements impacting the dormant repairable extras utilization. They utilize the BP neural system to estimate the utilization and consolidate it with a neural network algorithm which could streamline the weights and limits of the BP neural system. In Ref. [16], the examination plans to create, reference picture quality estimation calculations for JPEG pictures, and to arrange the picture in light of its quality an Elman neural system has been created. Another methodology utilizing the Modular Radial basis Function Neural Network (MRBFNN) strategy is introduced in Ref. [17] to enhance precipitation determining execution combined with suitable data pre-processing strategies by Singular Spectrum Analysis (SSA) as well as Partial Least Square (PLS) relapses.

Neural network dependent cloud computing for joint learning has numerous stages in that first client register on the cloud, then client upload the data into the cloud, When client transfers data to cloud data is ciphered by using AES algorithm, which implies a cipher content is transferred to cloud. As cipher content is transferred to cloud every learning procedure is done on the encrypted data as it were. Hence no client can realize whatever other clients information, and in this manner protection of various clients is stored. After that information from all clients is gathered for NN learning process, information is arbitrarily divided in to all clients. In arbitrary division there will be no restrictions like horizontal and/or vertical division, information is randomly divided as follows:

Divided information = Total gathered information/number of clients. Divided information is circulated among all clients, no client will be having same information set and after that scalar product is computed. After that a NN learning process begins, for learning NN a Back-Propagation algorithm is utilized. This calculation works in two stages Feed Forward as well as Back Propagation.

Feed forward Stage: 1. Initialize weights along with little, arbitrary qualities 2. While halting condition is not genuine for every preparation pair (input/output): each data unit shows its quality to every single concealed unit, each concealed unit sum up its information signals and applies actuation capacity to process its output signal each concealed unit sends its sign to the result oriented output units each and every output unit totals its info signals and applies its enactment capacity to calculate its output signal. Back propagation stag: 3. every output figures its error content, its own particular weight rectification term and its bias (threshold) rectification term and sends it to lower layer.4. Each concealed unit aggregates its delta input values from the above and duplicates by the subordinate of its enactment capacity; it too calculates its own weight adjustment term and its respective bias term signal. 5. Every output unit upgrades its weights and bias controlling the Weights. 6. Each concealed unit overhauls its weights and predisposition each preparation cycle is known as epoch. The weights are upgraded in every cycle It is not systematically conceivable to figure out where would be the global minima. In the long run the algorithm stops in a low point, which might simply be the local minima.

III. BACK PROPAGATION ALGORITHM

As appeared in Figure 1, the entire neural system is made out of three layers: first input layer, second hidden layer and third output layer. The accompanying strategy will demonstrate how the ANN (Artificial Neural Network) calculation works. Here are a few documentations utilized as a part of presenting the calculation: x, y, w represents the input information, output result, weight esteem separately, is rectification required just in the hidden as well as output layer, it will be persistently upgraded after every cycle, e is the error

esteem, is error gradient and p is the iteration number: 1) Initialization, set each of the weights and limit levels of the system to arbitrary

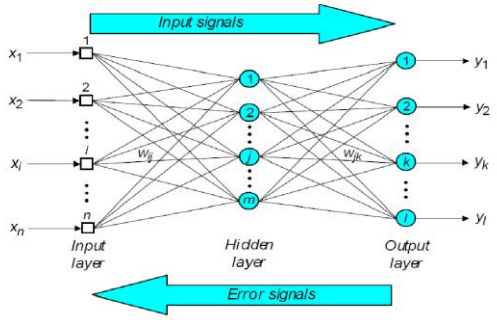

Fig1: General architecture of the back propagation algorithm based neural network.

Numbers consistently appropriated inside a little range (- 2.4/Fi, 2.4/Fi), where Fi is the aggregate of various inputs of a neuron i in the system. 2) Calculate the output of the neurons in the concealed layer 3) Calculate the genuine output of those neurons in that of output layer. 4) Compute the error slope for the neurons in that of output layer. 5) Computes weight rectification.

Various Encryption schemes for securing data:

Homomorphism Encryption (HE) scheme (Rivest et al., 1978) preserve some framework of the basic message space. Here, we accept that it gives techniques to add and to multiply encoded messages and thus protects the message storage area ring structure. We likewise expect that it could be utilized to work on the particular ring of integers. All things considered, messages are numbers and the plan saves the capacity to calculate summation as well as multiplication of such whole numbers. It is the Gentry (2009) the one who first to demonstrate that it is conceivable to build a Fully Homomorphic Encryption (FHE) plan, which implies that there will be no restriction on the degree of the p-polynomial and above. In hypothesis, this permits to assess discretionary calculations (since any calculation can be composed as a paired polynomial regarding parallel expansion and augmentation on the only one bits of the information). Indeed in spite of the fact that there has been incredible advancement in making FHE conspires more proficient and secure (see, for illustration, Brakerski and Vaikuntanathan (2014)), this methodology is presently not plausible for reasonable applications. Efficiency can be expanded by limiting to some degree homomorphic scheme as well as by working on numbers rather than bits, see Lauter et al. (2011). With this methodology, both the computational ambiguity as well as length of ciphertexts increment with the quantity of fancied operations carried out on the encoded information keeping in mind the end goal to ensure right unscrambling after polynomial assessment. While this expansion is generous while expanding the quantity of increments, it is more noteworthy while summing multiplication. In this way, an answer that expands upon these encryption plans must be limited to figuring low degree polynomials. In fact technically, (completely) homomorphic encryption takes into account a subjective number of summation and augmentation operations to be carried out on the scrambled. Information. For the purpose of effectiveness, we will rather utilize a weaker variation of this thought regularly called leveled homomorphic encryption,in which the parameters of the encryption plan are picked with the goal that number juggling circuits of (generally talking) a predetermined profundity can be assessed.

BGN Homomorphic Encryption: Homomorphic encryption empowers operations on plaintexts to be carried out on their individual ciphertexts without unveiling the plaintexts. Most available homomorphic encryption conspires just bolster single operation neither summation nor multiplication. Boneh et al. presented an open key doubly homomorphic encryption plan (called BGN in brief), which all the while bolsters single multiplication and boundless number of addition operations.

IV. VARIOUS SOLUTIONS PUT FORTH SO FAR:

Jiawei Yuan; Shucheng Yu.[1] Presents a back spread neural system learning algorithm is utilized for learning process across self-assertively divided information. As authors talked about back proliferation strategy is extremely proficient for training neural systems and here information is discretionarily apportioned means there is no restrictions for partitioning information like data is divided just on a horizontal plane or just vertically, it could be distributed either evenly or vertically. Here an answer is proposed for different gatherings, so the security of every clients private information is vital, for this reason they have actualized a security safeguarding multiparty BPN system learning algorithm. This strategy secures the private information of participants furthermore ensures the inter mediate results delivered amid the procedure of learning. To ensure the learning result about a protected scalar product calculation is utilized.

T. Chen and S. Zhong. [2] This paper represents a security protecting BPN system learning algorithm, however this algorithm is appropriate just for two gatherings. This algorithm gives a solid security to information sets and amid the learning process it secures the intermediate results. This technique is having restrictions like it quite supports two gatherings. This

strategy just supports vertically apportioned information. This technique is not versatile.

N. Schlitter.[3] Introduces a strategy for privacy entrusting BPN system learning, and permits two or many users to together lead Back Propagation Neural system learning. Amid this procedure private information of clients does not uncovered. As this technique permits many users, it requires confidential sum and secure grid expansion so for this reason a neural system grouping algorithm is utilized; this calculation is augmentation of Rumelhearts classification calculation. Here are a few restrictions, that the arrangement is given just for horizontal apportioned information, in the horizontal information each client have the same information composition, and every user holds a few records of aggregate information sets. This technique utilizes expansion of Rumelheart calculation which clearly does not ensure privacy. This strategy cant secure, intermediate results, produced amid the BPN learning process. To ensure the private information of participants, a protected calculation of inter mediate results is critical, in light of the fact that intermediate results likewise contains the sensitive information.

D. Boneh, E.- J. Goh, and K. Nissim [4] presents a 2- DNF equation on boolean variables. Consider F as a 2-DNF set of equation representation on boolean variables x1,...,xn. It represents a homomorphic open key encryption framework that permits the public assessment of F provides an encryption of the variables x1,...,xn. Or else provided the cipher texting of the binary digits x1,...,xn, anybody can make the encryption of F(x1,...,xn). Commonly, this has been assessed that quadratic multi-variate polynomials on encrypted text gave the subsequent resultant value merges inside of a little set. They exhibit various applications for this framework.

A. Bansal, T. Chen, and S. Zhong. [7] Presents an enhanced strategy and that provides an answer for information which is subjectively divided. In subjective apportioning of information, isolated information wont have particular order. This technique is very much similar to that of the strategy utilized as that of [2], which meant for vertically segment of information, and here it is for self-assertive segmentation of information. Here they attempted to extent the strategy from two users to multi party situation in any case, expansion of two users to multi party present calculation/communication ambiguity which is quadratic in the number of participants. In real time execution, such a multifaceted nature shows that of an enormous expense on every client.

Mrs.S.Blessy, Assistant Professor, AIHT, Indhumathi.S, Jayashree.R[19] showed that, Cloud processing permits their customers to share information.Various users might join through taking joint Back spread neural system learning on the combination of their individual information sets. Amid in this process none of the users desire to unveil her/his private information to others. Existing plans supporting this sort of community oriented learning are either constrained in the method for information segment or simply consider two users. There does not have a solution that permits two or more users, each with a self-assertively apportioned information set, to join the learning. Here they taken care of this open issue by using the capacity of distributed computing

V. CONCLUSION

Through this paper we will get a concise idea of understanding and analysing and cognizance about neural network based cloud computing platform for authentication of data through various encryption schemes and algorithms especially neural network based cloud computing back propagation techniques. Neural network and BP network plays crucial role in Joint collaborative learning and similar kind of cooperative process oriented tasks. More secure, reliable and user-friendly cloud computing is very most essential environment for upcoming Generations.

REFERENCES

[1] Jiawei Yuan; Shucheng Yu. ”Privacy Preserving Back-Propagation NeuralNetwork Learning Made Practical with Cloud Computing,” IEEE Transaction paper on parallel and distributedsystem, digital object identifier 2013 .

[2] T. Chen and S. Zhong. ”Privacy-preserving backpropagation neural network learning”. Trans. Neur. Netw., 20(10):15541564, Oct. 2009

[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] D. Boneh, E.-J. Goh, and K. Nissim. ”Evaluating 2-dnf formulas on ciphertexts”. In Proceedings of the Second international conference on Theory of Cryptography, TCC05, pages 325341, Berlin, Heidelberg,2005.

[5] A. Frank and A. Asuncion. ”UCI machine learning repository”, 2010.

[6] M. A. Inc. Amazon Elastic Compute Cloud (Amazon EC2). Amazon Inc., http://aws.amazon.com/ec2/pricing, 2008.

[7] A. Bansal, T. Chen, and S. Zhong." Privacy preserving backpropagation neural network learning over arbitrarily partitioned data". Neural Comput. Appl., 20(1):143150, Feb. 2011.

[8] SumitGoyal, Gyanendra Kumar Goyal,"Radial Basis (Exact Fit) Artificial NeuralNetwork Technique for Estimating Shelf Life of Burfi", Advances in Computer Scienceand its Applications (ISSN 2166-2924) 93 Vol. 1, No. 2, June 2012.

[9] SumitGoyal ,Gyanendra Kumar Goyal,"A Novel Method for Shelf Life Detection of Processed Cheese Using Cascade Single and Multi-Layer Artificial Neural Network Computing Models", ARPN Journal of Systems and Software, VOL.2, NO.2,February 2012.

[10] Kaushik Deb, Ibrahim Khan, AnikSaha, Kang-Hyun Jo,"An Efficient Method ofVehicle License Plate Recognition Based on Sliding Concentric Windows and Artificial Neural Network",2nd International Conference on Computer, Communication, Controla.nd Information Technology(C3IT-2012) on February 25 -26, 2012

[11] K.S. Kasiviswanathan, Avinash Agarwal,"Radio Basis Function Artificial Neural Network: Spread Selection", International Journal of Advanced Computer Science,Vol.2,No.11, pp. 394-398, 2012.

[12] Yuan Jing, Minfang, Qi, Zhongguang, Fu, "Prediction of coal calorific value based on the RBF neural network optimized by genetic algorithm", Natural Computation (ICNC),2012 Eighth International Conference, pp. 440-443, 2012.

[13] AnujaNagare, Shalini Bhatia, "Traffic Flow Control using Neural Network", International Journal of Applied Information Systems (IJAIS), Volume 1 No.2, January2012.

[14] PriyabrataKarmakar, Bappaditya Roy, Tirthankar Paul, Shreema Manna, "Target Classification: An application of Artificial Neural Network in Intelligent Transport System", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 6, June2012.

[15] Feng Guo, Su-qin Zhang, Deng-bin Zhang, Wei Gao, "Application of Genetic Neural Network on Lifeless-Repairable Spares Consumption Forecasting, Computer Science and Service System (CSSS)", 2012 International Conference, pp.1313-1315, 2012.

[16] Paulraj M. P, MohdShuhanazZanarAzalan, Hema C.R., Rajkumar Palaniappan, "Image Quality Assessment using Elman Neural Network Model and Interleaving Method", International Journal of Human Computer Interaction (IJHCI), Volume 3, Issue 3, 2012.

[17] Jiansheng Wu Yu, Jimin Yu, "Rainfall time series forecasting based on Modular RBF Neural Network model coupled with SSA