ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

Privacy Preserving ANN Learning Made Practical with Cloud Computing

Shinde Babaso A. , Ajay Gupta

M.E. Student, Dept. of Computer Engineering, IOK College of Engineering, Pimple Jagtap, Pune, India

Assistance Professor, Dept. of Computer Engineering, IOK College of Engineering, Pimple Jagtap, Pune, India

ABSTRACT: Back–propagation is very good and effective method for learning neural networking. This method is widely used various application. As compare to learning with local data set the collaborative learning is very effective to learn new things. The collaborative infrastructure like cloud computing the participating parties carries out learning not only their own data set, but also on other data set .The cloud computing is more convenient than ever for user across the internet. The user internet can shared all data without knowing with each other.
Beside of this advantage there one crucial issue pertaining to the internet-wide collaborative neural network learning is the protection of the data privacy for each participant. The participant in the cloud computing is from different trust domain and they may not Want to release their private data set which may contain proprietary information to anybody else. The solution shall be effective and scalable enough to support a random number of participants each processing arbitrarily participant data set.
Co-operative data sharing is an important aspect that is emerging heavily in cloud computing. This comes with a large risk of data leakage from the cloud. Thus a need for encoding data before storing on cloud becomes almost mandatory. But, in a multi owner data access structure it is important for clients to find mining results, to make any system function effortlessly. This paper supports architecture for storing data in an encoded manner on the server, yet making it feasible to apply ANN for mining on encoded data with an encoded query, which makes it impossible for a curious cloud owner to find and meaning of data, not even from the query.

KEYWORDS: Privacy reserving, learning, neural network, back-propagation, cloud computing.

I. INTRODUCTION

Cloud computing is emerging as the latest trend for IT field. cloud computing how business improves with the help of the information technology As a disruptive technology with profound implications, cloud computing is transforming the very nature of how businesses .Cloud is a place where information is stored which helps the clients users to use it as and when required Cloud is a user friendly system which is an innovation is this very 21st century. Now as the technology improves on the same side threat increases there is a need to avoid the threats to the data. It is in developing stage the ways to store data .The data stored in the cloud should be kept confidential between user and client .The data should not be misused by the service provider and the TPA Third party auditing. As users no longer physically possess the storage of their data, outmoded cryptographic primitives for the purpose of data security protection cannot be directly adopted.

The main objective is to provide security to the data that will be stored in the cloud. Presently the data stored in the cloud is been audited by third party. Now this data is available with the service provider .After a period of time even if the data is corrupted .It is not known to any one and the wrong data is forwarded to clients. This data is available where there is multiple users. Hence it's very important to have security to data. We would have to provide security to the data which we are going to store in the cloud .This comes in many ways by providing signature, by using encoding and decoding techniques etc. now a day's even the service provider are miss using the data even the TPA.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

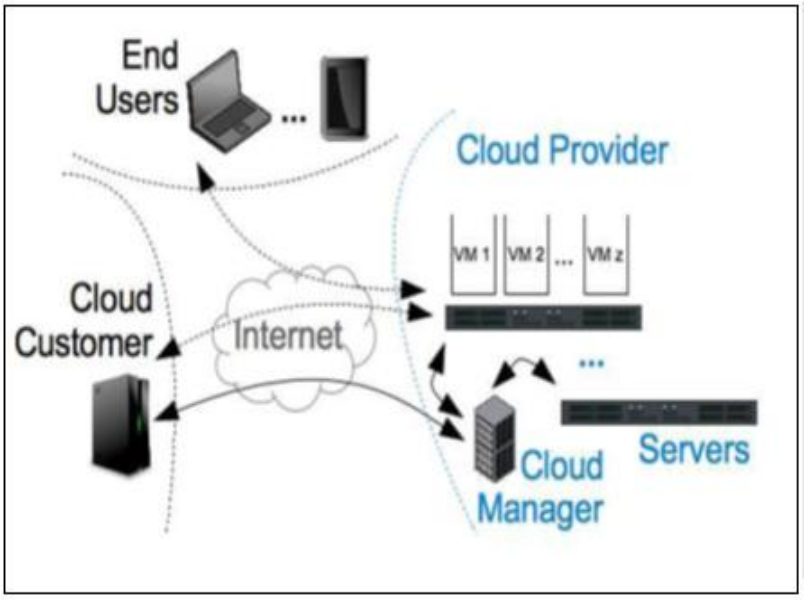


Fig 1: Architecture of cloud computing

II. LITERATURE SURVEY

Many of privacy preserving BPN network learning schemes have been proposed recently. N.Schlitter [4] introduces a privacy preserving BPN network learning scheme that enables how two or more parties are jointly perform BPN network learning without disclosing their private data sets. The limitation of this schema is that this schema is proposed only for horizontal partitioned data. The disadvantage of this schema is that this scheme cannot protect the transitional results, which may also contain sensitive data, during the learning process. To overcome this drawback Chen and Zhong [3] suggest a privacy preserving BPN network learning algorithm for two-party scenarios. This scheme provides strong security for data sets including transitional results. However, it just supports vertically partitioned data.

To overcome this limitation, Bansal. [2] Proposed a privacy preserving BPN network algorithms for two party scenarios. This scheme is provide solution for arbitrarily partitioned data. And providing protection for strong data sets including intermediate result.

Directly spreading them to the multiparty setting will introduce a communication complexity increases as increasing the number of participants. In applied implementation, such a difficulty represents a remarkable cost on each party considering the already expensive operations on the underlying groups such as elliptic curves.

From the previous base paper we can say that, none of present schemes have solved all these challenges at the same time. There still lacks an efficient and accessible solution that supports collaborative BPN network learning with privacy preservation in the multiparty setting and allows randomly partitioned data sets.

III. EXISTING SYSTEM

The existing system represents how data is stored and distributed on the cloud using partitioning to provide security and availability across two servers.

A.Client Side

a. File Selection

The user/users select a File to upload on the server.

b. Sending File

The client/clients sends respective file to Third Party Auditor (TPA) across the network using a File Transfer Protocol (FTP).

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

B. TPA

TPA performs six types of steps on the received file/files from the respective clients for storage across cloud with security and availability.

c. Receiving File

Third Party Auditor Receives File from the client/clients.

d. Partitioning File

TPA partitions file received from the client/clients.

e. Digital Signature Extraction

TPA extracts Digital Signature of each file partition.

f. Secret Key Generation

After partitioning, Third Party Auditor generates Secret keys for each partition respectively.

g. Encryption

TPA encrypts each partition using respective secret keys.

h. Storing Partition Sequence

TPA stores Partition Sequence, Signature, Keys and File attributes on its own server.

C. Server Side

i. Sending Partitions

Third Party Auditor sends the respective partition to the respective storage.

j. The Respective Storage Server receives the respective File from the Third Party Auditor.

k. Storing the storage server stores the partition received from the TPA.

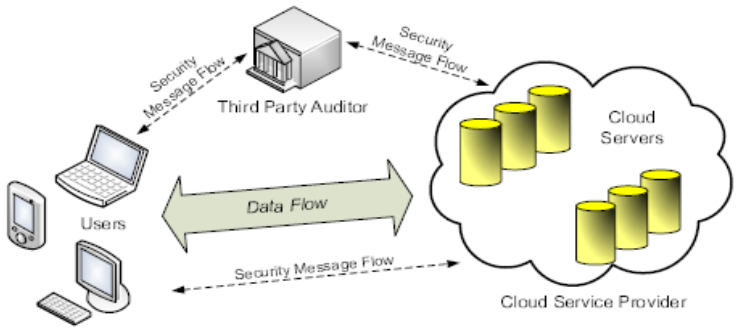


Fig.2. Partitioning and Domain Integrity Checking For Data Storage in Cloud Computing

IV. PROPOSED SYSTEM

The diagram shown above shows the proposed system. The system consists of end users, cloud server on which data to be stored.

1. The Authenticate user is login on his system.
2. After login he load the training data and encoding this data using scaling and transformation technique.
3. Then send this encoded data to server.
4. After receiving this encoded data then server train the data set using this data.
4. Then server will waiting for the test data from the user.
5. Then user loads the test data.
5. After receiving this test data to server the server can apply BPNN algorithm on the data. Then this data is stored

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

on the server.
6. User can retrieve this encoded data and decode this data using key.

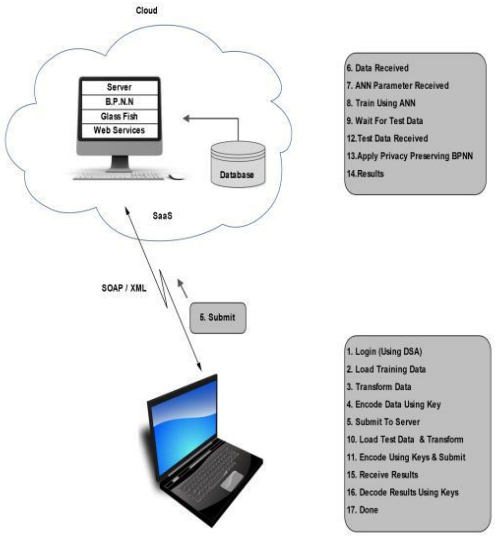


Fig 3: Architecture of proposed system

V. MATHEMATICAL MODEL

Let s (S) ≡ {U, T, DS, T', DS'}
Where,
U = {u1, u2, u3……un}
Where U is the infinite set of users.
T= {t1, t2,t3……tn}
Where T is a single transaction for H.D.
DS= {T1, T2, T3,……Tn}
Where DS is a set of data set including N no. of transaction.
T'= {t1', t2',….. …tn'}
Where T' is a single encoded transaction.
DS'= {T1', T2'……Tn'}
Where DS' is a set of data set including N no. of encoding transaction.

Functionalities:
U = Auth(uid, pass);
DS=load(transaction T);
DS'=encode(DS);
Send=sendToServer (DS');
RES'=train (DS');
Send'=sendToClient(Res')
Res=decode(Res')
Where,
Auth() = auth is a function to authenticate user parameters
parameters: uid,pass.
Load() =load function will import the dataset in application
parameters :Dataset file name.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

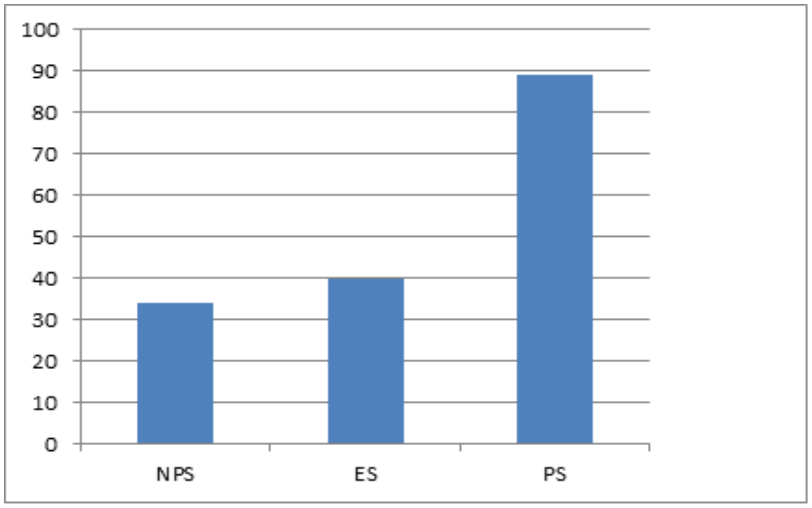
Vol. 3, Issue 11, November 2015

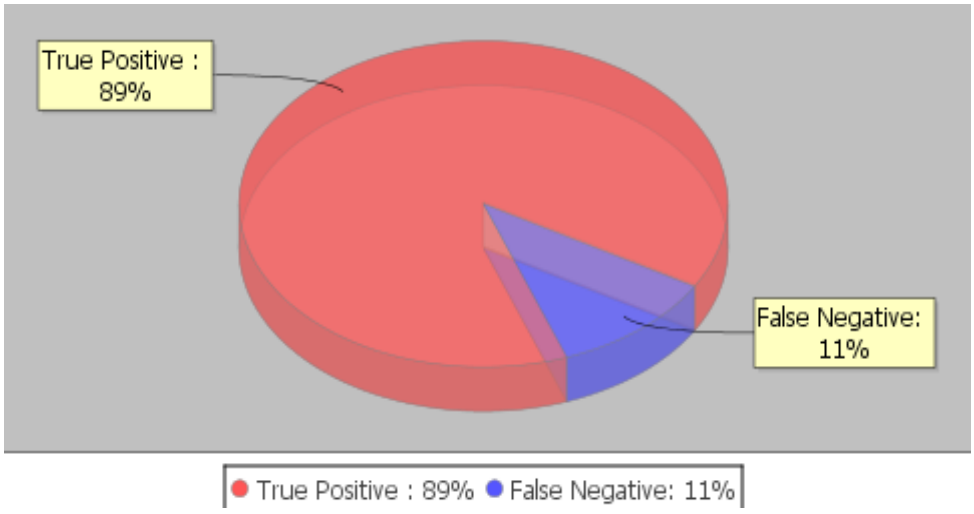
Encode() = encode function will convert the dataset to other format.
Parameters: imported dataset record.

SendToServer()
this function will send values to cloud server via networks.
Parameter : DS'
Train()
train function will apply ANN/FF/BPNN and train the network.
SendToClient()
This function send encoded result to the client.
Decode()
This function will give a original result of prediction.

VI RESULT

COMPARISON OF NON PRESERVING, EXISTING AND PROPOSED SCHEME





ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

VI. CONCLUSION AND FUTURE WORK

The Proposed system, we proposed the first secure and practical multiparty BPN network learning scheme over arbitrarily partitioned data. In our proposed approach, the parties encode their arbitrarily partitioned data and upload the encoded text to the cloud. The cloud can execute most operations relating to the BPN network learning algorithm without knowing any private information. The cost of each party in our scheme is independent to the number of parties. Complexity and security analysis shows that our proposed scheme is scalable, efficient, and secure. One interesting future work is to enable multiparty collaborative learning without the help of TA.

REFERENCES

1. Jiawei Yuan, Shucheng Yu, "Privacy Preserving Back propagation Neural Network Learning made practical with cloud computing"IEEE TRANS VOL. 25, NO. 1, JANUARY 2014.
2. A.Bansal, T.Chen, and S.Zhong. "Privacy Preserving Back propagation Neural Network Learning over Arbitrarily Partition data", Neural computing Application, vol20, no.1, pp.143-150, feb.2011.
3. T. Chen and S. Zhong "Privacy-Preserving Back propagation Neural Network Learning", IEEE Trans. Neural Network, vol. 20, no. 10, pp. 1554-1564, Oct. 2009
4. N. Schlitter "A Protocol for Privacy Preserving Neural Network Learning on Horizontal Partitioned data", Proc. Privacy Statistics in Databases (PSD '08), Sept. 2008.
5. Cong Wang, Sherman S.M. Chow, Qian Wang, V, Wenjing Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage". IEEE TRANS. VOL. 62, NO. 2, FEBRUARY 2013.
6. Fosca Giannotti, Laks V. S. Lakshmanan,Anna Monreale, Dino Pedreschi," Privacy-Preserving Mining of Association Rules From Outsourced transaction Database", IEEE SYSTEMS JOURNAL, VOL. 7, NO. 3, SEPTEMBER 2013.
7. Tinghuai Ma, Sainan Wang, Zhong Liu, "Privacy Preserving Based on Association Rule Mining,"2013.
8. Ning Cao, Cong Wang, Ming Li, Kui Ren, Wenjing Lou "Privacy-Preserving Multi-keyword Ranked Search over Encrypted Cloud Data,"
9. R.L. Grossman, "The Case for Cloud Computing," IT Professional,vol. 11, no. 2, pp. 23-27, Mar. 2009.
10. "The Health Insurance Portability and Accountability Act of Privacy and Security Rules," http://www.hhs.gov/ocr/privacy,2013.

BIOGRAPHY

Shinde Babaso A. has completed his graduation in Computer Engineering, University of Pune and perusing post-graduation in Department of Computer Engineering from IOK-COE, Pimple Jagtap, Pune. His area of interest includes the Cloud computing.