IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 12, Issue 2 (May. - Jun. 2013), PP 15-20
www.iosrjournals.org

Double Key Encryption Method (DKEM) Algorithms Using ANN for Data Storing and Retrieval in Cloud Computing

T. John Jeya Singh[1], Dr S.Jeya[2]
1(Asst Prof., MCA Department,Sambhram Academy of Management studies, Bangalore-97, India)
2(Professor & Head MCA. Department,Dayananda Sagar Academy of Technology and Management, Bangalore - 82, India)

Abstract: *Cloud computing is generally recognized as a technology which will have a significant impact on Information Technology in the future. The cloud computing data security has certain drawbacks in its implementation making it insecure. To avoid this problem in this research we propose enhanced security architecture for cloud computing using encryption and decryption system with double key cryptography based on Artificial Neural Network. The objective of the proposed scheme is to protect the information even if the hackers break the cipher text they can't convert cipher text to original text. In our proposed algorithms we have (training algorithm) adopted high data security authorized person can retrieve the data, including key generation, encryption and decryption that are provided in cloud computing system.*
Keywords: *Artificial Neural Network (ANN), cloud data storage Cloud data retrieval, decryption, encryption.*

I. Introduction

In the present day scenario almost all the organizations are trying to make an entry in to Cloud computing. The main advantages of cloud computing is cost saving, high availability and easy scalability. One must be very careful to understand the security risks and challenges posed in utilizing of these technologies [4].
Data security, which has always been an important aspect of quality service, traditional cryptographic primitives is used for the purpose of data security protection, which cannot be directly adopted due to the user loss control of data under cloud computing [2].

In order to store user's encrypted data, cryptographic storage is required in a cloud environment. The advantage of cryptographic storage is that no unauthorized users would be able to access the data [3] [6].
Cryptography is probably the most important aspect of data security and is increasingly important as a basic building block, for computer security. It is a study of how to protect the data in the computer and cloud where data cannot be accessed without authorization. Recent days, so many traditional encryption techniques such as Block cipher, DES algorithm, AES cipher, and RSA, Blowfish algorithm etc [7], are used. Along with these methods, the current researches in cryptography focus in Artificial Intelligence Techniques.

The security level is further increased, if necessary in cloud computing. We introduce new cryptography technology using artificial neural network based back propagation and symmetric key cryptography.
The main purpose and goal of employing this frame work is to ensure that confidential data is protected from potential attackers. This is done by guaranteeing data confidentiality and data integrity. This research proposes a new security mechanism that enhances the security of cloud computing.
The rest of the paper is organized as follows, after short introduction section II gives Literature Review. Section III describe in our proposed System followed by section IV, in which we give conclusion and future.

II. Literature Review

One basic research paper by Eva volna, Martin Kotyrba, Vaclav Kocian and Michal Janosek in Cryptography Based on Neural Network [8] was found to be a major source of motivation for forming the new concepts.

A paper entitled Applying Neural Network for simplified Data Encryption Standard (SDES) Cipher System Cryptanalysis [9] by Khaled Alallayah, Mohamed Amin,Waiel Abdelwahed and Alhamami was also found to be very useful in this regard.

Another one of the useful paper A comparative Survey on Symmetric Key Encryption Techniques [13] by Monika Agrawal and Pradeep Mishra was also found to use of symmetric key algorithms.

A paper entitled studding Enhanced Security Frame work to Ensure Data Security in Cloud Computing Using Cryptography [12] by M .Sudha and M. Monica was also found to very useful in this regard.

Another research paper by Chittaranjan Hota,Sunil Sanka ,Muttukrishnan Rajarajan and Srijith K Nair in Capability based Cryptographic Data Access Control in Cloud Computing [5] was found to be useful in this regard.

Another useful research paper Robust Data Security for cloud While using Third party Aditor [1] by Abhishek Mohta,Ravi Kant Sohu and Lalit Kumar Awasthi was also found to be very useful for third party auditor concepts.

Other useful book includes Cryptography and Network Security Principles and Practices [16] by William Stallings was also helped in this respect.

From the literature review it is clear that data security is the main issue of the cloud computing.

III. Proposed Scheme

In this section we describe Back Propagation Training or Learning Algorithm, Secret Key generation Algorithm using ANN, Data Storage, Data Retrieval and Benefits of our proposed System.

3.1. Back Propagation Network Training or Learning Algorithm

Artificial Neural Network is an interconnected group of artificial neurons that uses a mathematical model or computational model for information processing based on a connection processing based on a connectionist approach to computation[11].

The Back Propagation network is the training or learning algorithm. This algorithm aims to reduce errors backs wards from input to output. A back propagation network changes the network's weights, when training is finished, it will give required output for a particular input. This output is called Target. The input and its corresponding target are called a Training Pair.

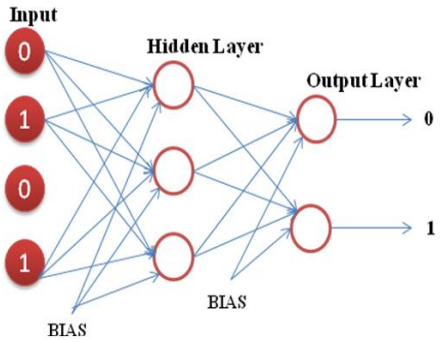

Fig. 1 Training Network

First this network initialized by the weights (Fig.1), weights it will tack small random values between -1 and +1.The input pattern is applied and the output calculated using this processing is called forward pass. Finally it will calculate the Error of each neuron.

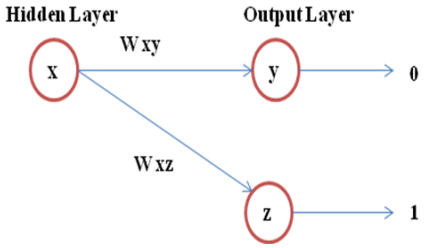

Fig. 2 A single connections Back Propagation Network

The connection between neuron x(Hidden Layer) and neuron y(Output Layer) and has the weight Wxy. The Fig. 2 also shows another connection x and z. But we have taken the first part. The Training Data Algorithm as follows.

To feed the input vector through the network. We are applying sigmoid function.

$$O = \sigma(\vec{w}\ \vec{x}) \quad (1)$$

$$\sigma(y) = \frac{1}{1+\epsilon^{-g}} \quad (2)$$

Calculate the squared error of the network.

$$E(\vec{w}) = \tfrac{1}{2} \sum y \in \text{outputs} (\text{target}_y - \text{output}_y)^2 \quad (3)$$

Calculate the error term of each output.

$$\delta y = \text{Output}_y (1-\text{Output}_y)(\text{target}_y - \text{output}_y) \quad (4)$$

Calculate the error term of the each hidden layer.

$$\delta_h = \text{output}_h (1-\text{output}_h) \sum y \in \text{outputs} w_{yh} \delta_y \quad (5)$$

Calculate the weight delts. Here eta is the learning rate. To speed up convergence we are using learning rate.

$$\triangle \mathbf{w_{ji}} = \eta \, \delta_j \mathbf{x_{ji}} \quad (6)$$

To add the weight deltas of each weights. We prefer adjusting the weights one layer at a time.

$$W_{ji} = \mathbf{w_{ji}} + \triangle \mathbf{w_{ji}} \quad (7)$$

By repeating this method we can train any number of layers.

3.2. Secret Key Generation Algorithm Using ANN

Cryptography is probably the most important aspect of security and is becoming increasingly important as a basic building block for computer security. Cryptography is now an emerging research area where the scientists are trying to develop some good encryption algorithm. The SSL (Secure Socket Layer) is support to encryption and decryption process in cloud computing [16].

The security for all encryption and decryption systems is based on a cryptographic key[8].A key is used to encrypt and decrypt the data. Modern cryptographic system include symetric key algorithms and Public key algorithms. Symetric key algorithms use a single shared key, keeping data secret requires keeping this key secret. Public key algorithms use two keys like public key and private key.A sender encrypts data with the public key only the holder of the private key can decrypt this data. Public key algorithms tend to be much slow than symmetric key algorithms. Symmetric key we can send information to more than one place.We are using Secret Key algorithm, the Secret Key generation algorithm as follows.

The network Weight to be initialized randomly with their hidden Weight (W) generated a random Secret Key.

$$\mathbf{K_o = r*w} \quad (8)$$

The same Key will not be used again for encryption purpose. The secret key algorithm to generate the keys (K_{oc} and K_{on})

C. Data Storage

One of the primary uses of cloud computing is data storage. Commonly known as Storage as a Service (StaaS), StaaS allows users to store their data at remote disks and access from any place at any time [10].Cloud storage service has many advantages [9].This service provide the users no need to install physical storage service in their own data center. We can get virtual storage resources, not only that it give data backup and data replication etc. The data is uploading to the cloud storage without leaving a copy in their local computers. The actual storage location may even differ from day to day or even minute to minute as the cloud dynamically manages available storage space.

Cloud Data Management Interface (CDMI) is provided with data path, create, retrieve, update and delete data elements from the cloud.

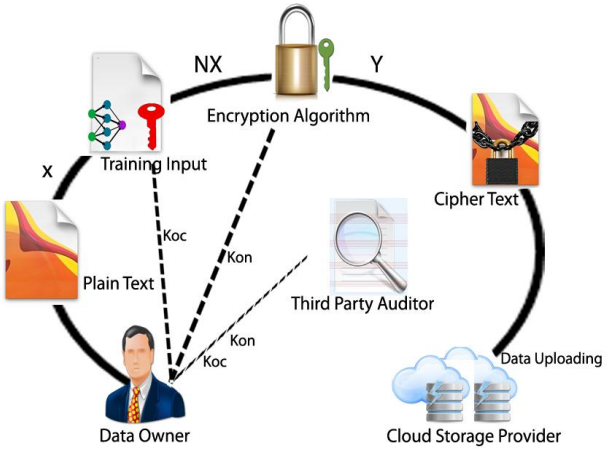

Fig. 3 The Architecture of Cloud Data Storage

In our proposed model we have two Stages (Fig. 3). The first stage uses plain text (X) and ANN input using transformation key (K_{Oc}) to produce the training input (NX). The second stage encrypted algorithm it will take training input and enciphering key (K_{On}) to produce Cipher text(Y). Enciphering keys use the different random weights, so the deciphering text that the intruder has received cannot be accumulated. Once the encryption process is completed the cipher texts are transferred to cloud storage. Then the center shares the keys with the third party auditor for future verification. The auditor can verify data, storage correctness and keeping the shared keys only. He can't modify or remove the data of his auditing [14].

The Data Storage and Encryption algorithm as follows.
A plain text X, with the transformation key k_{oc} as input, the plain text is converted to the ANN acceptable input NX where,

$$\mathbf{NX=TK_{oc}(X)} \quad (9)$$

Encryption algorithm accept the input NX, using enciphering key and its give cipher text output Y.

$$\mathbf{Y=EK_{on}(NX)} \quad (10)$$

Send the transformation key and enciphering key to data owner and Third Party Auditor (TPA). Data (Cipher text) uploading cloud server.

3.3. Data Retrieval

One of the main challenges in cloud computing data retrieval.The protocol RESTful HTTP is used to accessing the data and Meta data [15].

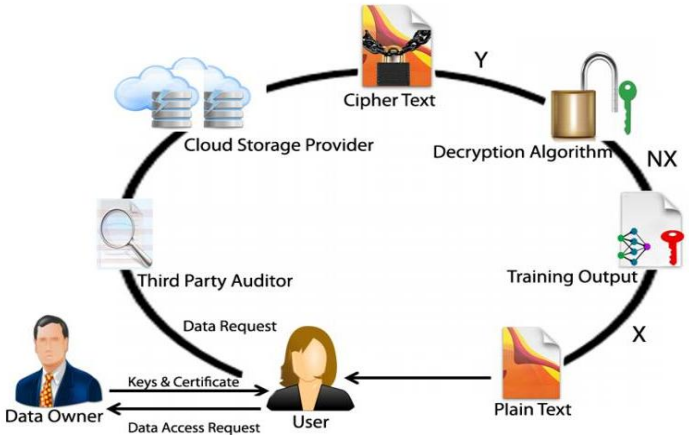

Fig. 4 The Architecture of Cloud Data Retrieval

In our proposed model (Fig. 4) the data owner given the keys and certificate to the user, the user asks the data request to the TPA. The TPA verifies the keys, if the keys match it will allow to take the cipher text (Y) from the cloud server. Firstly the decryption algorithm using deciphering key (K_{On}) it will make deciphering text (NX), Secondly ANN output using retransformation key (K_{Oc}) produce the original plain text (X) to the user.
The Data Retrieval and Decryption algorithm as follows.

User request to access a data from Third Party Auditor (TPA).TPA asks user for authentication keys (K_{on} and K_{oc}).TPA verifies authentication keys are correct send a request to Cloud Service Provider (CSP), the CSP sends a chipper text that you want to access.

$$\mathbf{Y=EK_{on}(NX)} \quad (11)$$

This decryption algorithm takes chipper text as a input using deciphering key give the output.

$$\mathbf{NX=DK_{on}(Y)} \quad (12)$$

This conversion algorithm takes output of decryption ANN as input and applies transformation techniques to generate the original plain text.

$$\mathbf{X=TK_{oc}(NX)} \quad (13)$$

The authorized user can receive the original data.

3.4. Benefits of our Proposed System

Our proposed model is high level secured because the training input adjusts their weights with trained data. Since our model easily and quickly gives final output, the plain text is encrypted easily and produces cipher text with less time. By using many numbers of hidden layers and nodes it increases the complexity of the ANN and thus provides more security of the cryptosystem. The training neural networks are acted as keys with their hidden weights. The key size is small. Our proposed model using symmetric key, symmetric key is faster than asymmetric encryption algorithm. The data stores cipher text in cloud. So even if the intruder hack the data, he can't decrypt. The data owners can have a strong confidence on their data which is secured safely on the cloud.

IV. Conclusion And Future Work

Cloud computing is one of the main technology in the information technology world. We believe this technology is facing many security challenges. Still many researches are on and many problems are yet to be identified. Our Aim is to develop Double key encryption technique using artificial neural network and symmetric cryptography algorithm. It provides high level speed and security in cloud environment. In the future we will try to find several possible better solutions using cryptography for this cloud computing.

References

Journal Papers

[1] Abhishek Mohta, Ravi Kant Sahu and Lalit Kumar Aswasthi, "*Robust Data Security for Cloud while using Third party Auditor*", IGARCSSE, Vol *2*, Issue *2* , February 2012.

[2] Annamaneni Samatha,Nimmala Jeevan Reddy and Pradeep Kumar "*Data Storage Collateral In Cloud Computing*",IJERA(International Journal of Engineering Research and Applications),Vol *2*,Issue *5*, pp1050-1055 Sep-Oct 2012.

[4] Arti Sharmaand Pawanesh Abrol, "*Cloud Computing Environment Problems Implementation*",International Journal of Computers and Distributed System,Vol *1*,Issues *3*,pp 64-68,October 2012.

[5] Chittarajan Hota ,Sunil Sanka,Muttukrishnan Rajarajan and Srijith K Nair, "*Capability based cryptography data access in cloud computing*", International Journal Advance Networking and Applications, Vol *3*, Issues *3*, pp 1152 – 1161,November 2011.

[6] Christian Henrich,"*Brief Announcement:Towards secure cloud computing*" Springer,LNCS 5873,pp 785-786,2009.

[7] Dinesh C Verma,A.K Mohapatra and Kaleem Usmani, "*Light Weight Encryption Technique for Group Communication in Cloud Computing Environment*",IJCA,Vol *49*,No *8*,pp 35-41,July 2012.

[8] Eva Volna , Martin Kotyrba,Vaclav Kocian and Michal Janosek,"*Cryptography Based on neural Network*", Proc 26th European on modelling and simulation ,ISBN:978-0-9564944-4-3, 2012.

[9] Khaled Alallayah,Mahamed Amin,Waiel AhdElwahed and Alaa Alhamami, "*Applying Neural Network for simplified Data Encryption Standard (SDES) Cipher System cryptanalysis"*, The International Arab Journal of Information Technology , Vol *9*, No *2*, PP 163-169, March 2012.

[10] L.M Kaufman, "*Data Security in the world of Cloud computing, Security & Privacy*", IEEE ,vol *7*, pp 61-64, 2009.

[12] M.Sudha and M.Monica, "*Enchanced security frame work to ensure data security in cloud computing using cryptography*", Advances in Computer Science and its Applications, vol *1*, No *1*,pp 32- 37, March 2012.

[13] Monica Agarwal and Pradeep Misra , "*A comparative survey on symmetric key encryption techniques*", IJCSE, Vol *5* , No *5*, PP 877 – 882, May 2012.

[14] Snsha Vijayaraghavan,K.Kiruthiga, B.Pattatharasi and S.Sathiskumar,"*Map-Reduce Function For Cloud Data Storage and Data Integrity Auditing By Trusted TPA*",International Journal of Communications and Engineering,Vol 05,No *5*,Issues *03*,pp 26-32,March 2012.

[15] Technical Position, "*Cloud Data Management Interface*", SNIA, Version *1.0.2*, June 4, pp 31, 2012.

Books

[3] Anthony T.Velte,Toby J.Velte ,Robert Elsenpeter "Cloud computing A Practical Approach" ,[Tata McGRAW Hill ,Edition 1], pp 157,[2009].

[11] Laurene V Fause "Fundamentals of Neural Neworks: Architure,Algorithms and Applications"[,Pearson Education,First Edition],pp 448-449,[1994].

[16] William Stallings,"Cryptography and Network Security Principles and Practices",[Fourth Edition,Pearson] ,pp 537,[2006].

About the Authors

T. John Jeya Singh has received Post Graduate degree and Master of Philosophy in the field of Computer Application. He is currently working as an Assistant Professor in the Department of MCA at Sambhram Academy of Management Studies, Bangalore, India. His areas of interest are Cloud Computing, Network Security and Artificial Neural Network. He has contributed numerous research articles in various journal and conferences. He has attended several workshops.

Dr. S. Jeya is currently working as Professor and Head, Department of Computer Applications in Dyananda Sagar Academy of Technology and Management, Bangalore. She received the B.Sc., M.C.A. and M.Phil., Degree in computer science from the Manonmaniyam Sundaranar University, Tirunelvelli, in 1994, 1997 and 2004 respectively, and the Ph.D. degree in computer science from Mother Teresa Women's University, Kodaikanal in 2010. She has sixteen years experience in teaching and research. She has published more than thirty five research papers in various international and national journals. Her research interests include network security, Data mining and image processing. She is a member of scientific and professional societies CSI, ISTE and IJERIA