A Predictive Model for Cloud Computing Security in Banking Sector Using Levenberg Marquardt Back Propagation with Cuckoo Search

Elliot, S J & Anireh, V.I.E (Ph.D), Nwiabu, N.D (Ph.D)
Department of Computer Science,
Rivers State University,
Port Harcourt, Nigeria.

Abstract

This study presents a predictive model for cloud computing security in the banking sector using Levenberg Marquardt Back Propagation algorithm trained with cuckoo search for fast and improved convergence speed. Object-oriented design methodology was used. The Levenberg Marquardt Back Propagation has been used to determine the training performance of an ANN, which is evaluated by computing the means square error of the system and that was the mean of the square of the difference between the target matrix and the input matrix. Cuckoo Search has been used to determine the weights of Neural Network. The signature feature vectors are input to the ANN; these features extracted from signature image were obtained via image processing. System was implemented in Matlab. Signature verification system based on the trained network was developed and tested with 160 signatures which consist of 90 genuine signatures,50 forgery signatures and 20 irregular signatures. The performance has been evaluated with False Rejection Rate of 0% and False Acceptance Rate of 8%.

Keywords: *Cloud Computing, Security, Artificial Neural Network, Levenberg Marquardt, BackPropagation, Cuckoo Search*

I. INTRODUCTION

Cloud security is a general subject but can be considered as any regulatory grouping, controls and technologies for protecting data, services and infrastructure from possible attacks or achieving business objectives with all the security domains working in an effective manner. Cloud computing has so many benefits, but in banking organisations, cloud computing is affected by numerous cloud security issues concerning application and program (software) security issues: authentication, authorisation, portability, insecure Application Program Interface (API), accessibility and mobility and interoperativeness[1].

Security of transaction is a major concern or threat confronting the web based businesses as well as the banking sector. Lack of safety can lead to serious damage, such as digital signature authentication problem. There are many ways to authenticate a user. The secure code generator is one form of verification which is a data-protection check against unauthorized user [12]. The system generates a code, the receiver does the same calculation and verifies the code to proof identity. The other form of verification is through Certification Authority (CA) with the sender's trust to check that the electronic currency or the digital signature they send is real

Thus, to deliver easy and stable banking transactions, digital signature authentication issue needs to be resolved. Many techniques have been used in solving security problems, among them are Artificial Neural Network. Back propagation training algorithm, however, is commonly used in artificial neural network techniques and is also a very common optimization method in finding optimal weight sets during training. Thus, traditional back propagation algorithms have some drawbacks such as getting stuck in local minimum and slow speed of convergence.

Reference[10] introduced Issues Faced by Banking Sector in the world of cloud-based computing to achieve high performance. They recommended that in a situation of security concern arising from the cloud computing, Hybrid Cloud should be used by banks for transactions, for highly secure transactions, a private cloud is used and for application's upper layer, a public cloud and kerberos for the purpose of authentication. Furthermore, they suggested Dynamic Firewall should

be used to defend attack by the intruder and Honey Pot for detecting unauthorized data use.

In managing and predicting cloud computing security performance, we use Levenberg Marquardt Back Propagation algorithm trained with cuckoo search. Levenberg Marquardt Back Propagation (LMBP) is a technique used in finding optimum network performance for training Artificial Neural Network (ANN). LM algorithm ranks as part of a highly effective training algorithm. Reference [6] proposed the use of Artificial Neural Network algorithm to predict critical cloud computing issues. They reiterated that cloud computing projects experience huge rate of failure especially if it involves financial housing. Despite having many advantages, there is need to beef up the cloud computing security problem. For this to be done successfully, identifying and addressing the issues early will help in the successful prediction. This study proposed a method that combines Levenberg Marquardt algorithm and Cuckoo Search (CS) to train neural network to solve these security issues in cloud computing.

II. RELATED WORKS

Reference [5] discussed on the Security of Today's On-line Electronic Banking Systems. Online banking security's most critical issue is to safeguard vital information that is susceptible to attackers' unauthorized access. The banks must therefore constantly increase their protection.

Reference[2] proposed applicable conceptual cloud computing Security framework for banking industries. They wrote that concerns relating to services in banking such as regulatory, legal, compliance, privacy and security needed be addressed. They used the Sherwood Applied Business Security Architecture(SABSA) enterprise security technique as a standard to design security framework recently recommended. The drawback of this method is that it is a complex business procedure and is resistant to change.

A. Artificial Neural Network (ANN)

Artificial neural network, as a connectionist system, is a model for processing of information, motivated by the way biologic nervous systems, like the brain, processes information. ANN are aggregated into layers that may perform different type of transformation on their input. There are training algorithms used in ANN. These include Gradient Descent, Conjugate Gradient, Newton's Method, Quasi Newton Method and Levenberg Marquardt Back Propagation (LMBP) [11].

Reference [3] proposed that the artificial neural network has emerged as a key tool for addressing the issue of the nonlinearity of energy building data and the efficient computation of large and dynamical data.

B. Levenberg Marquardt Back Propagation (LMBP)

Levenberg Marquardt Back Propagation (LMBP) training algorithm. Is a commonly used neural network technique and is also a common optimization task in finding the optimum weight range during the training process. The drawback of LMBP is that its convergence speed is slow and it gets trapped in local minima.. It is rated as a training algorithm that is highly effective for small and medium sized pattern. It's used for training neural network where the output index is measured in Mean Square Error but can not stop local minima.. In order to overcome this problem, cuckoo search(CS) is used for fast and improved convergence speed. It combines with LMBP algorithm to train neural network for XOR dataset.

Reference [9] applied Artificial Neural Network (ANNs) with Levenberg – Marquardt algorithm for an hourly prediction, in advance of (IT) and (IH) in hot-humid-area buildings showing outcome certifying that ANN could also be for hourly IT and IH prediction usage.

C. Cuckoo Search Method

Cuckoos adopt an aggressive strategy of parenting; Their eggs are laid in the nests of host bird's.. To do this, they look for nests that have eggs very close in colour to theirs. They do this ensure hosting bird does not differentiate between the eggs belonging to it and the cuckoo's. When time goes by and Cuckoo's baby is brought forth, it struggles to push out the hosting bird's eggs in the nest [4]. Cuckoo Search (CS) is a population-based metaheuristic algorithm inspired by the parenting behaviour of the bird cuckoo. [13].

Reference [7] presented Cuckoo Search Algorithm - Web Service Composition (CSA-WSC), which was gradually developed on the basics of CS algorithm structure. They used the Cloudsim toolkit to consider the WS QoS (Quantity of service) and the QoS network. The simulation results indicate that in terms of QoS parameters, we can produce near-optimal results.

III. METHODOLOGY

The research methods adopted are Constructive Research Methodology and Object-Oriented Design Methodology.

A. Proposed System Design

The system being proposed makes use of online efficient Artificial Neural Network techniques; it is continuously learning which is extremely good in predicting the performance of cloud computing security

on customer's signature verification in banking organization. Figure 3.1 represents architectural design of the proposed system. The Levenberg Marquardt Backpropagation (LMBP) algorithm estimates accuracy of performance when predicting cloud security levels. The cuckoo search finds the best solution by getting the weight of the neural network.

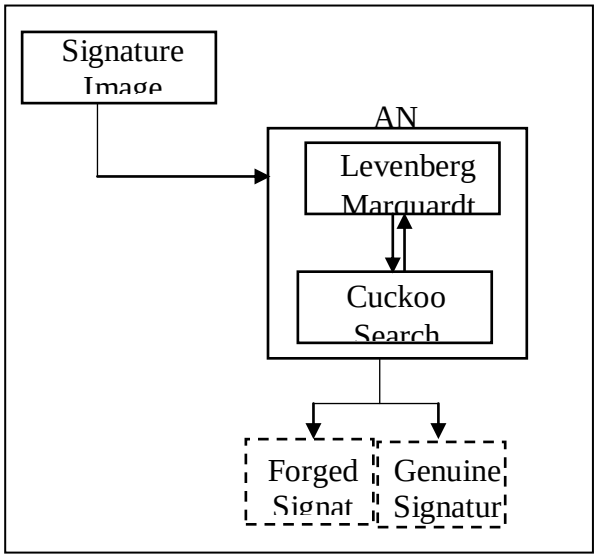

Figure 3.1: Architecture of the Proposed System

a) Input Variables

The input to the system is the customer's signature. Signature samples may be collected by uploading the hard copy of the signature. Before signature verification can be achieved, it must pass through training procedure.

b) Application of Artificial Neural Network

The three layers Neural Network is represented in Figure 3.2.The neural network consist of input layer, an output layer, with one layer hidden between the input and output layers. The first is input layer. Set input value X denotes the customer's signatures. Every node in the input layer has a X_i signal as network input, multiplied by a weight (W) value between the input layer and the hidden layer and produces Y which is the output.

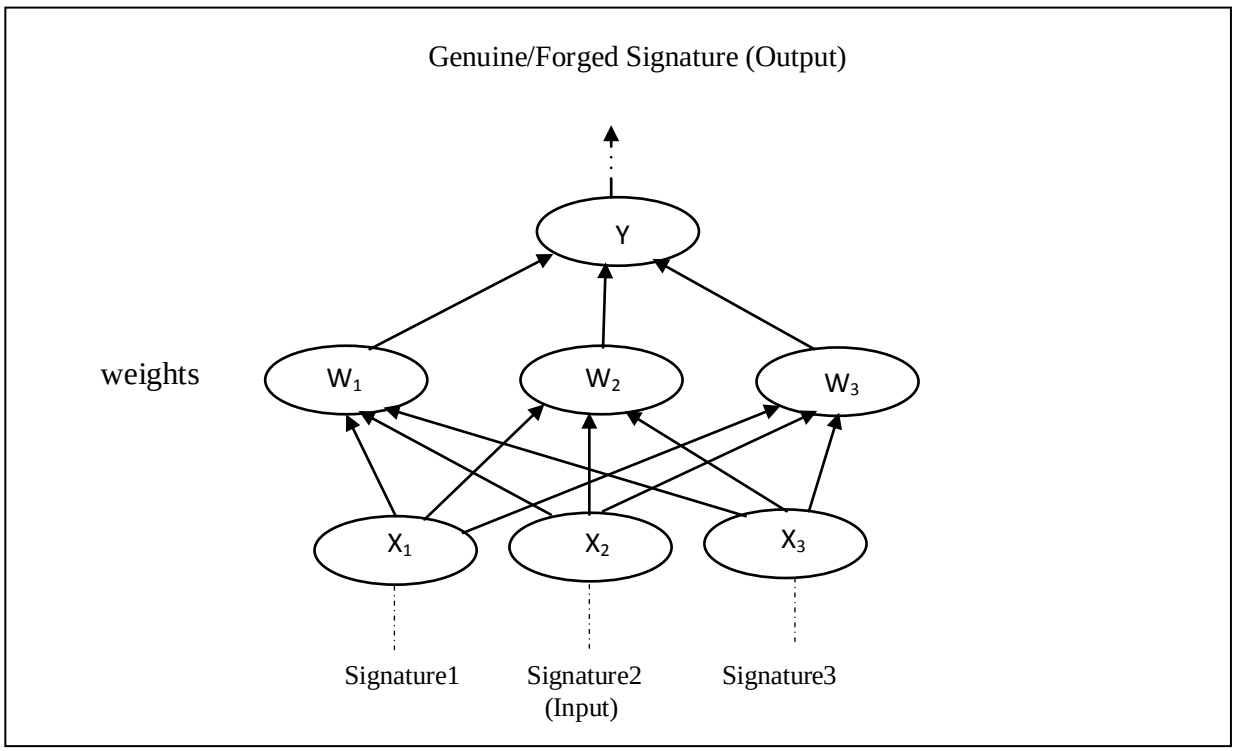

Figure 3.2: Neural Network of the System.

c) Levenberg Marquardt Backpropagation (LMBP)

Training performance of an ANN is evaluated by computing the means square error of the system and this is computed as the mean of the square of the difference between the target matrix and the input matrix. The training is done by the system. In carrying out ANN training, the system uses Levenberg-Marquardt Back-propagation algorithm.

The target matrix is a matrix of low input and high input data and is given as follows:

$$MSE = \frac{1}{N}\sum_{j=1}^{N}(p_j - b_j)^2 \quad (3.1)$$

Where,
MSE is the Mean Square Error
N = number of iterations, there is no optimal number for iteration. The system iterates until the error is significantly reduced.
P_j= target outputs, which is the target feature vector
b_j= input b, which is the feature vector to be calculated.

In carrying out ANN training, the system uses Levenberg-Marquardt Back-propagation with mathematical model given as follows:

$$y_{k+1} = y_k - (J^t J + \mu)^{-1} J^T \quad (3.2)$$

Where,
y_{k+1}= output matrix
y_k= input matrix
T= target matrix,
e= errors,
μ = scalar
J = Jacobian Matrix.

d) Cuckoo Search

The weight of the neural network were calculated using Cuckoo Search. The method starts with an initial population by random and the population changes with each iteration via Cuckoo Search. Each individual shows Artificial Neural Network's weight.
The system's accuracy is obtained as:

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (3.3)$$

$$Genuine = \frac{TP}{TP+FN} \quad (3.4)$$

$$Forged = \frac{TN}{TN+FP} \quad (3.5)$$

Where,
TP is the number of correctly identified Signatures
FP is the number of incorrectly identified Signatures
TN is the number of correctly rejected Signatures
FN is the number of incorrectly rejected Signatures

B. Experimental Detail

The testing procedure is outlined as follows:

1. Start Matlab
2. Load the main application file (pre-process_testdata, pre-process_traindata, signature CSLM.m, cuckoo_search_spring.m)
3. Click the run button for the following:
   (i) Click the signature CSLM.m, the result of the bestnest will appear.
   (ii) Click the cuckoo_search_spring.m the neural network training (non traintool) will startup
   (iii) Go to the performance to see the plot perform and record the generated file from plot regression.
4. Read and record the output from the Matlab work space
5. Exit the Matlab.

IV. RESULTS AND DISCUSSION

The security check in banking sector is achieved through signature verification. Customer's data is gotten online. The features of the signature images are obtained through image processing. During image processing, the original signature is acquired and converted to binary image. The input and target data (desired output) is loaded into the ANN in a metric column. One hundred and sixty signature samples were used in Artificial Neural Network; five signature attributes were use in each. In the CSLM-ANN, the node number of input is 4, 10 hidden layer nodes and 160 output layer. The MSE training error is 0.10906. The testing error is basically closed with 0.10984. The best validation performance is 0.11 at 70epoch (iteration) out of 76 epochs.

The performance accuracy of the system in predicting cloud security level in banking sector has been estimated using False Acceptance Rate (FAR) and False Rejection Rate (FRR) as shown in Table 4.1.Total number of 160 signatures which consists of 90 genuine, 50 forgery and 20 irregular.

Table 4.1: Signature Performance Rate

Type of Signature	No of Signatures	Accepted Signatures	Rejectd Signatures	FAR	FRR
Genuine	90	90	0	0%	0%
Forgery	50	4	46	8%	92%
Irregular	20	8	12	40%	60%
Total	160	102	58	48%	152%

The genuine, forgery and irregular signatures were evaluated using false rejection rate and false acceptance rate as depicted in Figure 4.1.y-axis represents FAR and FRR. x-axis represents types of signature.

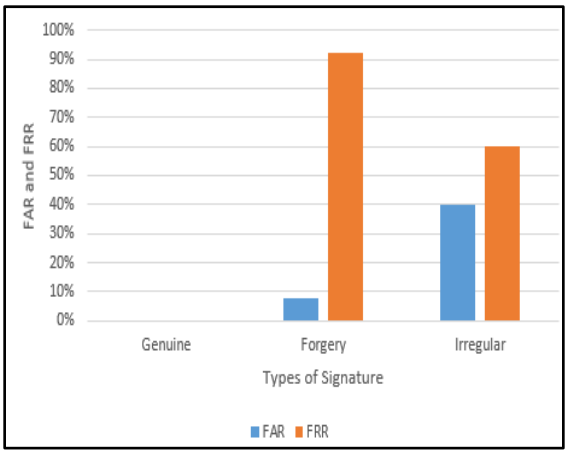

Figure 4.1: Representation of FAR and FRR of Signature

A. Training Result

The training result of CS best weight and its effect on LM training is presented in Table 4.2.

Table 4.2: Training Result

No. of Training	CL (BESTNEST)	LM			EPOCHS
		Training error	Testing error	Validation error	
1	8.4521	0.10906	0.10984	0.11	76
2	0.4175	0.10320	0.10321	0.10468	31
3	0.05410	0.10247	0.10401	0.10365	38

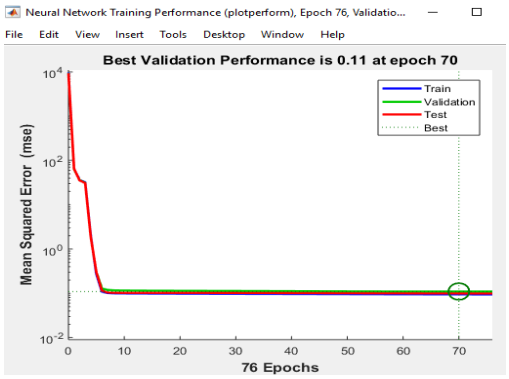

Figure 4.2: CSLM Line Graph

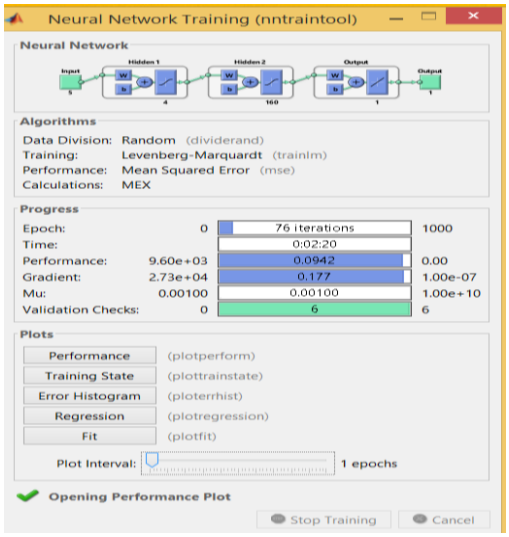

Figure 4.3: Neural Network

B. Comparison Analysis

The proposed CSLM algorithm has better performance than existing systems Levenberg- Marquardt (LM) and Artificial Bee Colony Levenberg- Marquardt (ABCLM)) with validation 0.11. Hence, CSLM produces better result than LM as show in Table 4.3.

Table 4.3: Comparison with Existing System

Models	Training Error	Testing Error	Validation	Epochs
LM	4.94160	1.95378	8.7581	7
CSLM	0.10906	0.10984	0.11	76
ABC-LM	4.95202	1.95442	8.7511	100

V. CONCLUSION

This study implemented predictive model for cloud computing security in the banking sector using Levenberg Marquardt Back Propagation algorithm trained with cuckoo search. Prediction of cloud computing security in the banking sector is of great importance as successful prediction may boost security strength of many companies. The signature feature vectors are input to the ANN; these features extracted from signature image were obtained via image processing. The system security level further increased as password encryption is affected. The system performance is good and can be traced to the CSLM algorithm and feature vector used. This system can replace the manual signing of signature.

REFERENCES

[1] Al-anzi, F., Yadav, S. and Soni, J. (2014).Cloud Computing: Security Model Comprising Governance, Risk Management and Compliance. In International Conference on Data Mining and Intelligent Computing (ICDMIC), 1–6.

[2] Alemu, M. and Omer, A. (2014).Cloud Computing Conceptual Security Framework for Banking Industry.Journal of Emerging Trends in Computing and Information Sciences, 5(12), 2079-8407.

[3] Biswas, M. A. R., Robinson, M. D. and Fumo, N. (2016). Prediction of residential building energy consumption: a neural network approach. 117, 84–92.

[4] Chifu, V. R., Pop,C. B., Salomie, I., Suia, D. S. and Niculici, A. N. (2012).“Optimizingthe Semantic Web Service Composition Process Using Cuckoo Search.

[5] Claessens, J., Dem, V., Cock, D., Preneel, B. and Vandewalle, J. (2002). On the Security of Today's On-line Electronic Banking Systems.Computers and Security 21(3), 253-265.

[6] Elzamly, A., Hussin, B., Abu-Naser, S. S., Shibutani, T. and Doheir, M. (2017).Predicting Critical Cloud Computing Security Issues using Artificial Neural Network (ANNs) Algorithms in Banking Organizations.International Journal of Information Technology and Electrical Engineering, 6(2), 2306.

[7] Ghobaei-Arani, M., Rahmanian, A., Aslanpour, M. and Dashti, S. (2017). CSAWSC: Cuckoo Search Algorithm for Web Service Composition in Cloud Environments. Soft Computer.

[8] Mba, L., Meukam, P. and Kemajou, A. (2016).Application of artificial neural network for predicting hourly indoor air temperature and relative humidity in modern building in humid region.EnergyBuild, 121, 32–42.

[9] Modak, M. and Walke, A. (2013). Issues Faced by Banking Sector in The World of Cloud based Computing to Achieve High Performance: A Survey. International Journal of Advances in Computer Science and Cloud Computing, 1(1), 2321-4058.

[10] Mukhopadhyay, S., Tang, C., Huang, J., Yu, M. and Palakal, M. (2002).A comparative study of genetic sequence classification algorithms. Neural networks for signal processing. In Proceedings of the 12th IEEE workshop, 57–66.

[11] Pfleeger, C. P. (1997) Security in Computing. Prentice Hall, 2(5)..

[12] Yang, X. S. and Karamanoglu, M. (2013). Swarm Intelligence and Bio-Inspired Computation: An Overview. Elsevier, 243-255.