

AUTHENTICATION SCHEME USING TREE PARITY ARTIFICIAL NEURAL NETWORKS FOR FRAUD DETECTION IN AN ON-LINE BANKING SYSTEM

¹Hammed, M. & ²Adesi, A.B.

^{1&2}Department of Computer Science Federal Polytechnic Ilaro, Nigeria E-mails:
mudasiru.hammed@federalpolyilaro.edu.ng; adesiadesolabolaji@gmail.com

Abstract

Internet usage has increased drastically and provides many opportunities such as shopping either online or offline using various facility provided by bank e.g Credit Card, Debit Card, Internet Banking are also possible. But, one of the major problems in the banking is that the way in which adversary and unauthorized users have been gaining access bank resource. However, many studies have proposed numbers method to rapidly detect and identify intrusion in banking transaction. But, unauthorized users are still gaining access to bank resources. This study proposed Tree parity artificial neural network authentication system to detect fraud in banking transaction. The system has been tested with 500 student and 450 student were successfully login with correct password. But, only 50 student were unable to login due to wrong password. This shows that the system is efficient to detect fraud in banking transactions.

Keywords: *Authentication scheme, Tree parity, artificial neural network, Online banking*

1.0 Introduction

Today technology is basic mandatory need of human (Krishna and Lata, 2013). There are lots of advantages of technology, but with that it causes fraud (Krishna and Lata, 2013). One of the biggest facility provided by technology is that shopping either online or offline using various facility provided by bank e.g Credit Card, Debit Card, Internet Banking are possible (Linda, 2009). But, it is a major chance for fraud. Fraud is a behavior of human which is out of rule and causes crime (Krishna and Lata, 2013). With the rapid growth of Internet, computer attacks and intrusions are increasing and can cause financial loss to an organization or an individual. The number of malicious applications targeting internet banking transactions has increased severely in recent years (Pritika, 2015). The fraud/ intrusion represent a challenge not only to the customers who use such facilities, but also to the banking institutions which offer them. Detection of intrusions or fraud is an important issue during internet banking and e-commerce transactions (Pritika, 2015). Intrusion detection systems aim at identifying any entity that attempts to compromise the confidentiality, integrity or availability of a computing resource (Adetunji, *et. al.*, 2014). Different intrusion detection systems have been proposed by numbers of researchers as an efficient solution to protect online financial systems against intrusions and other attacks. Literature revealed that fraud in banking system increasing as there is rapid growth of internet usage. This study proposed three parity artificial neural networks authentication scheme as a solution to detect fraud in banking transactions.

2.0 Literature Review

The Tree Parity Machine (TPM) consists of an artificial neural network with one unit in the output layer and K Units in the hidden layer. Each hidden unit takes N inputs. We can label the weights of the hidden units. The weight takes an integer value. L is the synaptic depth. For Tree Parity Machines to be able to converge during mutual learning it necessary that $L < 1$ which simply means that the synnaptic depth is bounded. Weights are not drawn from a random pool of numbers, they are randomly initialized and the process of synchronizing involves in sorting of random walk of each and every weight within the range. Mutual Learning of Tree Parity Machines proceeds as follows. With respect to a hardware implantation, it is important to note only signs and bounded integers which are processed within the algorithm. The result of outer product can be realized without multiplication. The sign of the weight only changes the sum within the product.

2.1 Related Works

Tieming and Samuel, (2008), proposed One-Time Password (OTP) was used as the strongest authentication scheme among all password-based solutions. Recently, user devices such as smart card have implemented OTP based two-factor authentications for secure access controls. Synchronization of internal parameters in OTP models, such as moving factor or counter, between the client and server is the key challenge. Recently, it shows that two interacting neural networks, Tree Parity Machine with common inputs can finally synchronize their weight vectors through finite steps of output-based mutual learning. The improved Tree Parity Machine can be utilized to synchronize parameters for OTP schemes. Two TPM based OTP was introduces, one is the implementation model including initialization and rekeying while the other is light-weight and efficient suitable for resource constrained embedded environment.

Diplomarbeit, (2012), proposed the implementation of a successful probabilisticattack to crack a Neural Cryptographic system. Neural Cryptography has been developed during the last decade with great success. Two systems implemented on artificial neural network have shown to be robust enough askey-exchange protocols when tested against different attacks.A probabilistic attack attempts to track the probability that the key-exchange protocol is converging towards each possible secret key and is radically different from those attacks tried before on Neural Cryptography. Permutation Parity Machine(PPM)as a described algorithm shows an outstanding performance which an be concluded that the system is not safe enough for any cryptographic means. The Tree Parity Machine (TPM) are only of a speculative nature and do not allow assessment of the security of the system under such an attack.

Raihiet. *al.*, (2004), proposed a type of smart devices called USBKey has been used to secure user identifications and authentications. USBKey based OTP authentications depend on two-factor implementations built in hardware. A one-time password is firstly calculated as $pwd_1 = H(K, C)$ by the USB token and sent to the server; afterwards the value of counter C is

incremented by one. Meanwhile, the authentication server calculates the one-time password by the same way and compares with that from the client. If the password matches, the authentication succeeds and the server counter C is also incremented simultaneously for synchronizing with that of the client. However, it is a little awkward for counter resynchronization every time the client fails to connect to the server. In that case, it is possible that the client counter works but the server is unaware of it. In other cases, updating the shared secrecy K may also be compromised. The Tree Parity Machine (TPM) are only of a speculative nature and do not allow assessment of the security of the system under such an attack.

3.0 Methodology

3.1 Tree parity artificial neural network

The tree parity artificial neural network for fraud detection in banking transaction as it is shown in figure 1 consists of the following layers:

INPUT LAYER: This layer comprises of the User ID and password.

HIDDEN LAYER: This layer of the study comprises of the three aspects which are password, generation of pin by confirming it in the register user email and also security question for confirmation

OUTPUT LAYER: After the complete processing of the registered user and confirmation of being the full owner of the account, the user will perform his/her intended transactions.

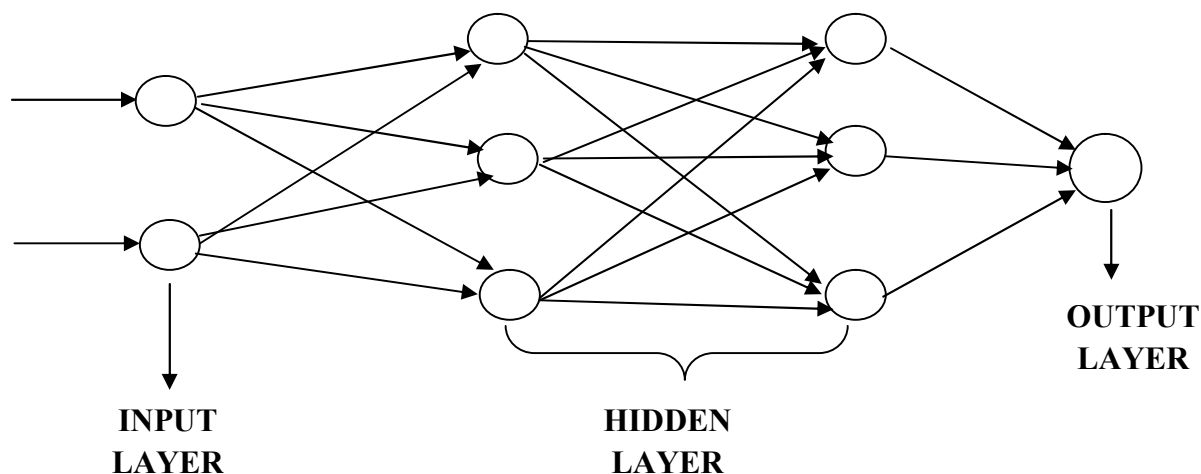


Figure 3: Tree parity artificial neural networks architecture

This study used tree parity artificial neural networks to authenticate every user that wants to perform transaction especially withdrawal of cash using cards. The system stores details information of every customer such as name, address, phone number, email address, account number and card number. It also stores the password used by the user during registration. Before a customer can be activated to perform transaction, the system will first check the customer's details and match the patterns corresponding to the user password. If any significant deviations is not detected then one time personal identification number (PIN) alongside with a security

question will be sent to the customer as another means of authenticating the customer. If significant deviations were not being detected then the customer will be activated and otherwise, the customer will be deactivated. The diagram in figure 1 depicts fraud detection system and the diagram in figure 2 depicts the flow of information in the system.

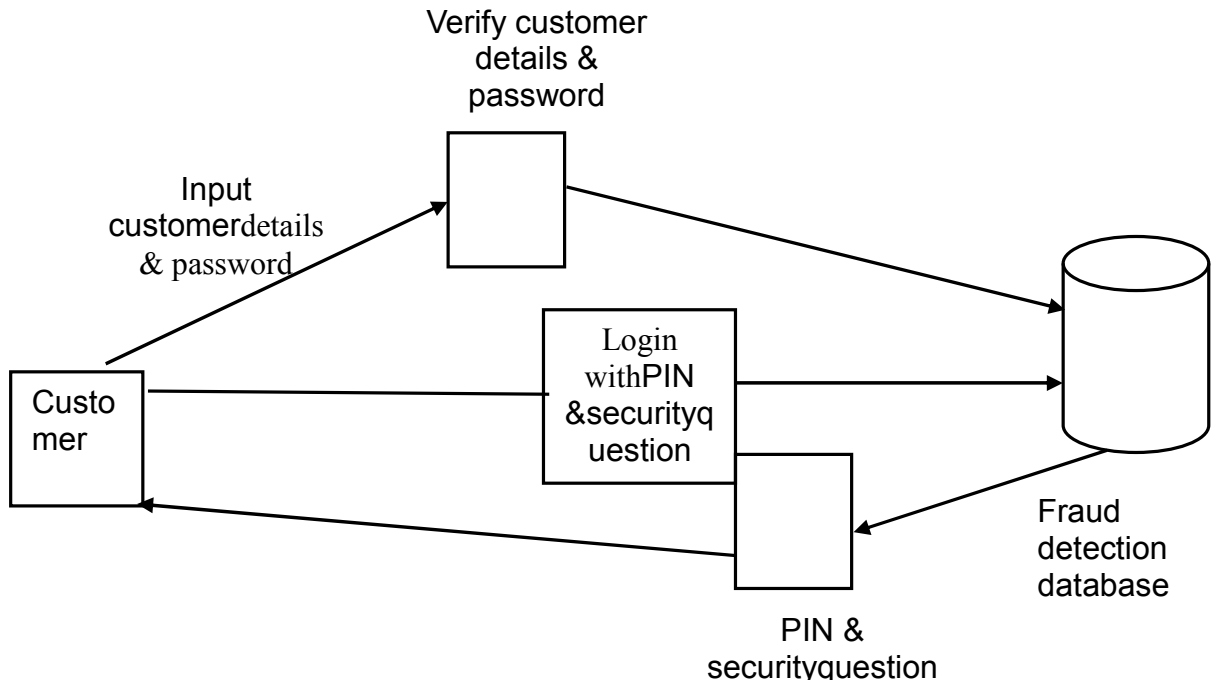


Figure 1: The System Design

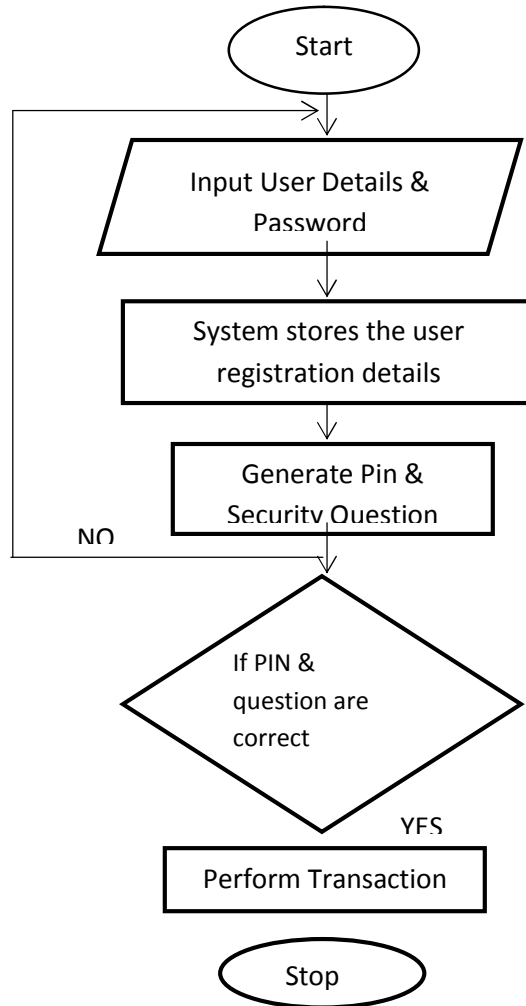


Figure 2: The Flowchart Design for the System

3.2 Discussion

When the site is launched, the homepage will be displayed, which is the web page that will be initially shown whenever the site is being logged on to. The system is a dynamic website which dynamically displays its information accurately.

It is implemented offline by hosting it on the local host to accomplish its purpose. The efficiency of this project is well recognized in the On-line banking system for fraud detection.

This program is divided into three main sections:

1. Sign in Page.
2. Sign up page.
3. Main menu.

Sign Up page

This is the page where the user can register in order to be able to login. Each user has to register before they can be granted the access to login and view the main page of the software. Figure 4 shows the page where customers can sign up to register for any online transaction.

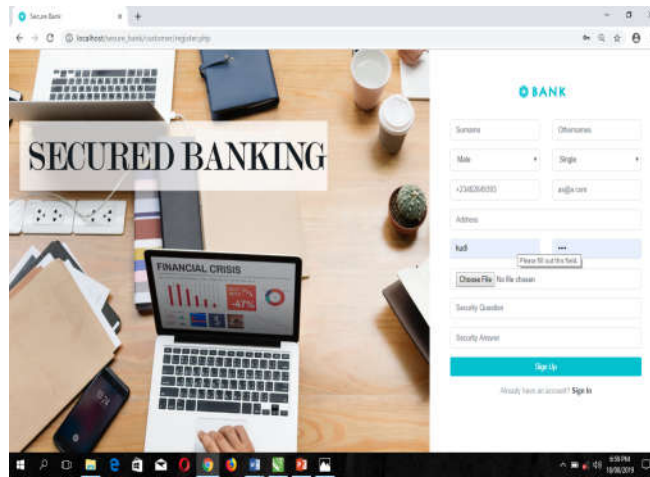


Figure 4:Sign up Page (Registration for new user)

Sign in Page

This is the first section to be seen when the software is loaded on the screen, it is a page where the user with successful registration can log into their account. It requires the user to input the right username and password in order to gain access to the main menu and utilize the powers of the On-line banking system. Figure 5 depicts the page where customers will login for subsequent transaction after the registration.

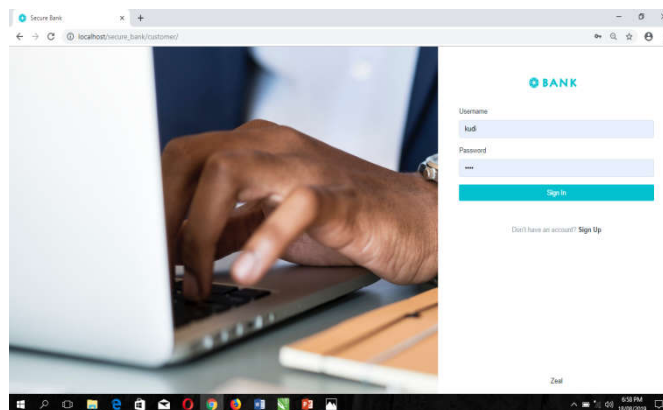


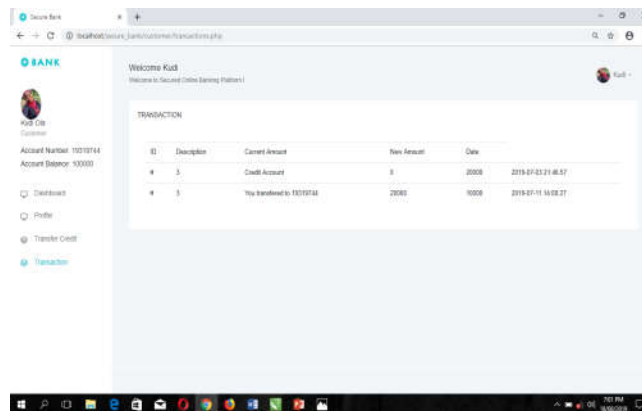
Figure 5:Sign in Page

Main Page

The main page also includes other pages whose navigation menus are by the side of the main menu. The menu includes;

- i. **User Dashboard:** This display the user account number, total amount, transaction made, total money transfer (Debit) and total money receive into the account(credit)
- ii. **Profile:** Where the user can view the inputs made during the registration in the sign up page and also upload of image is allow.
- iii. **Transfer Credit:** This displays occur the when the user needs to make transfer and will also requires to answer the security question and also a pin which will be already sent to the email the user registered with.
- iv. **Transaction:** This display all the transactions made including the amount, date, and destination.

The figure 6 depicts the result of a successful transaction when customers login into the system.



The screenshot shows a web browser window with the URL 'securebank.com/customer/transaction.php'. The page is titled 'Welcome Kudi' and shows account details for 'Kudi Oki Customer' with account number '1010114' and balance '10000'. A table of transactions is displayed:

ID	Description	Current Amount	New Amount	Date
1	Credit Account	0	2000	2019-07-21 08:57
2	You transfer to 1010114	2000	1000	2019-07-11 16:08:27

Figure 6: Page shows successful transaction

3.3 Result

This system has been tested at Federal Polytechnic; Ilaro, Computer the system authenticated 500student, 450student were successfully login with correct password. Only 50student were tested with wrong password but, they were unable to login. This shows that the system attained a high degree of accuracy.

Conclusion

The implementation of Tree parity artificial networks system in an On-line Banking transaction System for fraud detection. It aimed at reducing fraud, theft, confidential and securing user account. The system was tested and it attained high degree of accuracy.

References

- Adetunji A.B, Ayinde A.Q and Akanbi C.O., (2014). Application of Neural Network to Detect Intrusion in Banking System, *American Journal of scientific and industrial research*, 5(2): 53-59.
- Krishna, K. T. and Lata, R. (2013). Hybrid Approach for Credit Card Fraud Detection, *International Journal of Soft Computing and Engineering (IJSCE)*,3(4), 8- 11.
- Pritika, M., (2015). Controlling Attacks and Intrusions on Internet Banking using Intrusion Detection System in Banks, *International Journal of Advanced Research in Computer and Communication Engineering*, 4(11). 346- 348.
- Linda, D., (2009). Credit card fraud and detection techniques: *a review*”. *Bank and Bank Systems*, 4(2).
- Tieming, C. and Samuel, H. H., (2008). Tree Parity Machine-basedOne-Time Password, InternationalJoint Conference on Neural Networks (IJCNN) IEEE 2008, 257- 261.
- Diplomarbeit J.O (2012). Bernstein Center for Computational Neuroscience of the Technical, *University of Berlin, Publication*.
- Raihi,D.M., Bellare,M., Hoornaert,F., (2004). HOTP:AnHMAC-basedOneTime Password Algorithm , *IETF Network Working Group, RFC draft, Oct. 2004*.

