International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391

Fraud Detection in E-Transactions using Deep Neural Networks - A Case of Financial Institutions in Zimbabwe

Elliot Mbunge[1], Ralph Makuyana[2], Nation Chirara[3], Antony Chingosho[4]

[1, 2, 3, 4]Chinhoyi University of Technology, School of Science and Engineering, Department of ICT & Electronics, Chinhoyi, Zimbabwe

Abstract: ***Due to advancement in E-Commerce, the most common method of payment is credit card for both online and offline. It has become the most convenient way of online shopping, paying bills and money transfers. Hence, the credit card industry is investing vast amounts of money to secure credit card transactions. Financial institutions that have adopted credit card as a payment method are prone to credit card fraud attacks. The objective of this study was to develop a distributed application that analyses financial datasets to detect the possibility fraudulent activities in financial transactions. The researchers used the Hidden Markov Models (HMM) to analyze the datasets so as to generate the spending profile of a cardholder. The results generated from the HMM are then fed into the Multilayer Perceptron (MLP) that classifies the transaction into suspicious and non-suspicious classes. Since the researchers could not obtain a real dataset from the bank, one that resembles a bank dataset has been developed to train and test the MLP.***

Keywords: Fraud, Credit card, E-Commerce, Deep learning, Multilayer Perceptron, Hidden Markov

1. Introduction

Fraud is defined as unlawful deception which results in monetary gain [1]. Since e-transactions are done without the physical present of the cardholder, fraudsters find it easy to manipulate and falsify authentication process to gain unauthorised access. Smart card, Credit card, Electronic Fund transfer, Debit Card and electronic money are basic mode of electronic payments [2] . Most electronic payments are done by using credit cards. Credit cards are vulnerable to fraud due to weak authentication and authorisation process [3]. Credit cards use two factor authentication and authorization process – what you have (credit card number) and what you know (Personal Identification Number) [4]. Technology is evolving such that two factor authentication is becoming susceptible to fraudsters through advanced social engineering [5] and man-in –the-middle attacks [6].

Electronic payments has made financial transactions much easier in Zimbabwe.This is triggered by shortage of hard cash in circulation that has led to cash crisis [7]. In the first quater of the year 2017, payments through electronic payment platforms recorded 70% all of transactions made [8] which shows that the countrt is operating on plastic money platform. Credit cards are being used in bank Automated Teller Machines (ATM) to withdraw money against the credit limit extended to the cardholder. In Zimbabwe, electronic technologies emerged in the early 1990s, with industry leaders like Standard Chartered bank and Barclays Bank PLC [9]. However, cyber credit card fraud is a continuing danger that can befall individuals who use credit cards. According to Aihua et al.[10], external card and inner card fraud are generally two types of credit card fraud. Inner credit card is facilitated by bank employee and cardholder to defraud the bank. Inner credit card is facilitated by bank employee and cardholder to defraud the bank. External credit card fraud occur when an intruder uses the stolen, lost, and counterfeit card to falsify the bank and have unauthorised access to money.

The extent of credit card fraud is difficult to quantify; this is due to the reason that financial institutions loath to disclose information to the public domain regarding fraudulent activities as it tarnishes the image of the institution and it also provides an opportunity for fraudsters to exploit the security measures with the intention of circumventing them. However, available sources reveal that credit cards have been the target of fraudsters. For instance, fraud cost consumers more than $16 billion in the United States of America [11], bank merchants lost US$190 billion in 2011 [12] and UD$8 billion lost in credit card fraud in 2016 [13]. Zimbabwe is not an exception when it comes to fraudulent money transfers over electronic payments. Records reveal that most of the financial institutions in Zimbabwe have suffered fraudulent money transfers. Machakaire [14] reported that a trainee customer service officer with FBC Bank connived with a bank teller and swindled the Ministry of Mines more than $500 000. Rupapa [15] reported that a manager with Steward Bank defrauded the bank of over $180 000 by creating fictitious credit accounts that he used to purchase air tickets, withdraw cash as well as buy goods in foreign countries.

As technology advances, new techniques are being developed to counter credit card fraudulent activities. Complex algorithms, mathematical models and statistical models have been used to detect fraud in money transfers that involve credit cards.

2. Research Objectives

To design and develop an application that analyses financial datasets to detect the possibility of credit card fraud transaction using deep neural networks techniques..

3. Research Question

How to design and develop an application that analyses financial datasets to detect the possibility of credit card fraud transaction using deep learning Hidden Markov model

4. Computational Techniques Applied

Several computational intelligent techniques have been used to develop intelligent applications that mimic how the human brains make reasonable decisions in new or known environment. In this study, researchers used deep neural networks computational techniques to develop an artifact.

4.1 Transaction parameters considered are;

a) Amount of money to be withdrawn
This is the amount of money that a cardholder specifies when performing a withdrawal transaction. In this particular study, the researchers will refer to this withdrawal amount as amount. Each cardholder has a unique spending behavior; this is reflected by the variations in total amount of transactions. This depends on several factors like monthly income of the cardholder, nature of activities the cardholder engages in and financial responsibilities of the cardholder. For example, a cardholder may have a spending pattern of ($200, $120, $80, $180, $110)

b) Time Taken to Perform a Transaction
This is the time taken by the cardholder from the moment when the system accepts a correct PIN from the cardholder up to the time when the cardholder presses ACCEPT button to submit details for a transaction to be processed. The time varies from one cardholder to another since there are many operations that can be done, for example checking balance, changing PIN or cash transfer before withdrawing money. In this research, this variation in time is used to model a profile for each cardholder to identify anomalies, which can point to suspicious activities on the account.

c) Location of ATM
Normally cardholders perform transactions in particular locations. This information can be inferred from the dataset and can be used to identify particular locations where a cardholder regularly performs transactions. With this information, anomalies can be identified with the intention of pointing suspicious activities on a particular account. In this research, location of ATM is referred to as location.

d) Day of the month
A cardholder performs his/her withdrawal transactions on particular dates within a month. For example, an account can be active, in terms of withdrawal transactions, within the first week of the month or the last week of the month. This data can be modeled to form a cardholder's profile, which can be used to identify anomaly activities on the account. For example, a transaction is tagged suspicious if it is performed within the last week of the month on an account that reflects regular transactions within the first week of the month. In this research, this variable is represented as day.

e) Time of the day
A cardholder performs his/her most withdrawal transactions with a given range of time of the day. For example, a cardholder can usually perform a transaction during the day.

The researchers could have divided the day into four, that is, early morning (12am to 5:59am), morning (6am to 11:59am), afternoon (1200pm to 5:59pm) and evening (6:00pm to 11:59pm)

This data could have been modeled to form a cardholder's profile, which can be used to note deviations. For example, a transaction is tagged suspicious if it is performed in the evening on an account that reflects regular transactions in the afternoon.

4.2 Deep neural networks computational techniques implemented are;

4.2.1 Genetic algorithms
Genetic algorithms use evolutionary techniques to solve difficult computational tasks [16]. Ramakalyani & Umadevi [17] used genetic algorithms to detect fraud in the electronic payment systems to avoid sending false alerts to the merchants and cardholder. Securing the e-payment gateway does not eliminate the possibility of fraud to occur but it only encrypts e-transaction details. In this study, the researchers have considered the customer buying and spending behavior as a key element to detect the possibility of fraudulent activities, that is, any mismatches are considered suspicious. The parameters that have used include: number of times the card is used, location where transaction are made, the rate of spending, the balance available in the account and the average daily spending amount.

4.1.2 Hidden Markov Model (HMM)
Hidden Markov Model is the probabilistic sequence model: given a sequence of unites, HMM compute a probability distribution over possible sequences of labels and choose the best label sequence [18]. In this case, three different spending profiles are considered depending on price range, named high, medium and low. The price ranges are as follows: low ($0-$100), medium ($100-$500) and high ($500 up to card limit). The HMM parameters are estimated for each cardholder as well as initial sequence of the existing spending behavior of the cardholder. This sequence is inserted in HMM to compute the probability of acceptance, which forms the basis for telling whether a transaction is fraudulent or legitimate.

Hidden Markov Model uses probability distributions to determine or predict the likelihood/possibility of an event occurring given a finite set of sequential events. Normally, the model is trained to generate initial probabilities denoting the likelihood of a transition from one state to another. These probabilities will form what is known as the Transition Matrix (T). This matrix is made up of transition probabilities that represent the probabilities of moving from one state to another. The model can be trained when object involved in the process are clustered. This is done so as to generate a value that represents a particular cluster. However, such generalization can reduce the accuracy of the system. In this

research, accounts have not been clustered rather the model is used to generate a profile for each accountholder. Hence, training of the model has not been done since the data is fully observed; all data for a particular account holder is in the dataset. This data is modeled to generate the transition probabilities as follows:

a. Amount

In this research amount has been divided into three categories, which are low (L), medium (M) and high (H) – L ($10-$290), M ($300-$490) and H ($500-$1000). This means that at any time, a particular account can be in an L state or M state or H state. These states formulate the sequence of states for the variable amount and can be used to observe the sequence in modeling the accountholder's profile

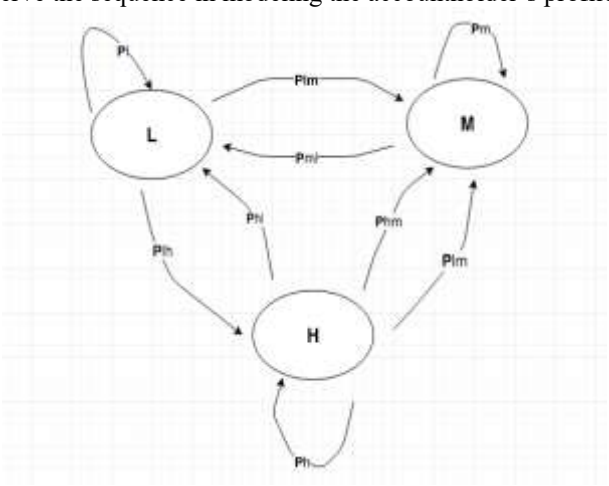

Figure 1: Transition Diagram – Amount Variable

Steps for finding Transition Probabilities

Step 1: Determine the total number of transactions (T) performed on a particular account from the dataset. T represents this value.

Step 2: Determine the state (L, M, H) of the recent transaction performed on that particular account.

Step 3: Identify the state (L, M, H) of the current transaction being performed on that particular account. Step 4: Note the transition from *Step 2* to *Step 3*. This can be L-L, L-M, L-H, M-M, M-L, M-H, H-H, H-L or H-M. Then calculate the frequency of transition probabilities. For example, to calculate the likelihood of a transaction P_{hm} (a transition from High amount to Medium Amount), the following procedure is taken:

$$PA = (P_{lm}, P_{ml}, P_{mh}, P_{hm}, P_{lh}, P_{hl}, P_l, P_m, P_h) / T \quad (1)$$

Instead of making a decision a final decision from PA, it is fed into the Multilayer Perceptron (3.4 below) as input 1($\mathbf{X}_1$) in the input layer.

b. Time

The researchers have categorized the time variable into short (S), average (A) and long (L) –L (0-20), A (21-40) and L (40+). The transition diagram for the variable time with states; S, A and L is as shown in Figure 2.

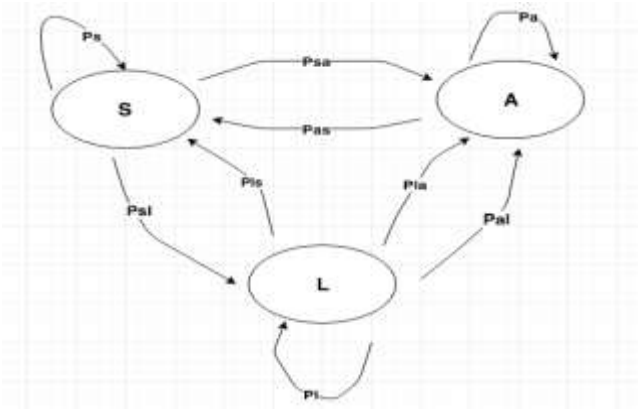

Figure 2: Probability Transition Diagram-Time variable

This means that at any given time, considering the time variable, the account can be in any one of the states in the Figure 2. Hence, the same procedure for calculating the transition probabilities as in amount variable (3.3.1 above) is used for the time variable. Thus, P_t is calculated as follows:

$$\boldsymbol{P_t} = (P_{sa}, P_{as}, P_s, P_{ls}, P_{sl}, P_l, P_{al}, P_{la}, Pa)/ \boldsymbol{T} \quad (2)$$

Hence, P_t becomes the second input to the MLP (section 3.4) and is represented by $\mathbf{X}_2$

c. Day

In this research, days of the month have been categorized into four weeks, that is week one (WK1), week two (WK2), week three (WK3) and week four (WK4) – WK1 (day 1 to day 7), WK2 (day 8 to day 14), WK3 (day 15 to day 21) and WK4 (day 22 to day 31). These categories form the states for the variable day

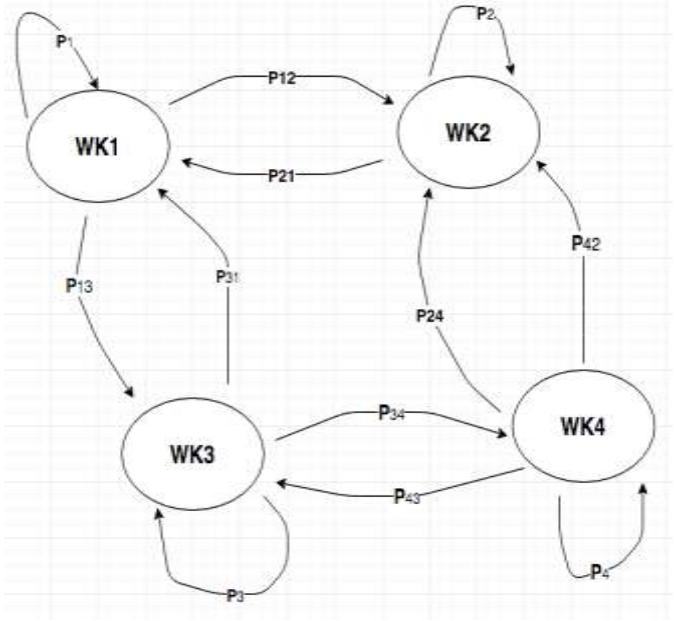

Figure 3: Probability Transition diagram -Day variable

A transaction can fall into any one of the four states. To determine the transition probabilities, the researchers have followed the same approach. Hence, the probability of a transaction being performed in a particular week is calculated as follows:

$$P_D = (P_{12}, P_{21}, P_1, P_{23}, P_{32}, P_2, P_{34}, P_{43}, P_3, P_{41}, P_{14}, P_4)/T \quad (3)$$

Hence, P_D becomes the third input to the MLP (section 3.4) and is represented by $\mathbf{X}_3$.

d. Location

In this research, which is based on financial institutions in Zimbabwe, ATMs have been grouped according to the province they belong and each ATM is given a Unique Identification (ID). In this research, the location of a transaction is inferred from the ATM ID on which the transaction is performed. To calculate, P_L – the probability of a transaction being performed on a particular location, the total number of transactions (T) is calculated first. Then the total number of transactions (t) performed in that particular location is determined. This is given by the following formula:

$$\mathbf{P_L = t / T}. \quad (4)$$

This means that PL becomes the fourth input to the MLP (section 3.4) and is represented by $\mathbf{X_4}$.

4.1.3 Deep Neural Networks

Deep Neural Network (DNN) is characterized by a particular structure that allows them to learn and adjust so as to provide an optimal solution to the problem. It is made up of neurons that are organized in successive layers. Deep Neural Networks consist of interconnected neurons that are inspired by human brains [19]. These neurons perform some mathematical computations using inputs from input layer and activation function. In this case, researchers used feedforward Multilayer perceptron which consists of input layer, hidden layer and output layer - processing of input data in only in one direction.

In this particular research, a Multilayer Perceptron (MLP) is used to classify transaction into two categories i.e. suspicious (S) and non-suspicious (¬S).

MLP used has the following layers;

i. Input layer

This layer is responsible for accepting inputs into the system for computation. In this research, it is made up of four nodes that accept four inputs (X_1, X_2, X_3, and X_4) as input vector. This input vector is generated from the Hidden Markov Model as a matrix of probability distributions.

ii. Hidden layer(s)

Two hidden layers have been used to perform mathematical computation using four inputs from input layer. The second hidden layer uses outputs of the first hidden layer as inputs to solve to classify transaction.

iii. Output layer

This layer is normally constituted by output values of the linear combination of the functions of the hidden layer. This layer has two nodes to denote S and S-.

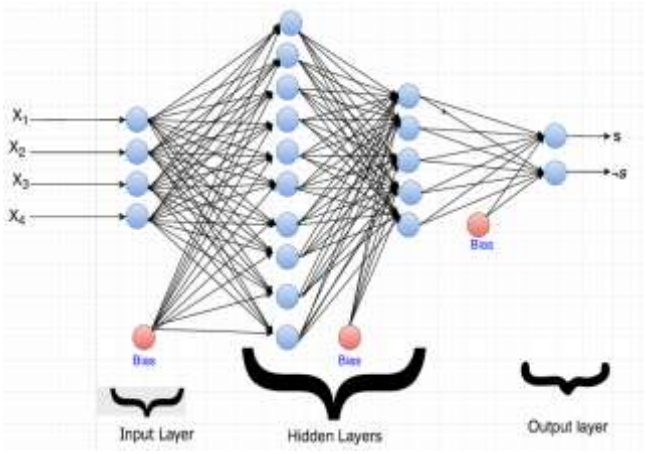

Figure 4: Multilayer perceptron

DNN network training

Differentiable sigmoid activation function is used for mathematical computation in the hidden layer and output layer [20]. Sigmoid activation function solves non-linearly separable. The network uses supervised learning algorithm-BackPropagation learning algorithm to train the network [21]. Online financial dataset was used as a training set - to train the network. Dummy financial dataset was used as the validation or testing set to measure performance of the network. Online financial dataset was used as a training set. BackPropagation learning algorithm requires both fraudulent and non-fraudulent training samples to construct the models that used for transaction classification purpose.

DNN decision phase

The decision, whether a transaction is suspicious (S) or non-suspicious (S-), is made from the output of the MLP. If the transaction is suspicious, the system generates a token (one-time-password) and sends it to the mobile number corresponding to the account on which the transaction has been performed. One-Time-Password (OTP) is valid for 60 seconds. This means that the cardholder performing the transaction should provide the token within 60 seconds so that the transaction can be authorized, otherwise the account is blocked. If the transaction is non-suspicious, the system will allow the transaction to proceed as normal.

4.1.4 Verifying a transaction with One-Time Password

The researchers used Ozeki Short Message Service (sms) gateway to send and receive OTP using HTTP Request Protocol. In addition to that, the researchers used Telerivet API to send the SMS from the system (Credit card Fraud Detection System) to the Telerivet Cloud Servers. These servers are responsible for formatting the SMS from the developed Credit card Fraud Detection System (CFDS) and send it the recipient with the mobile phone provided. This is shown in Figure 5.

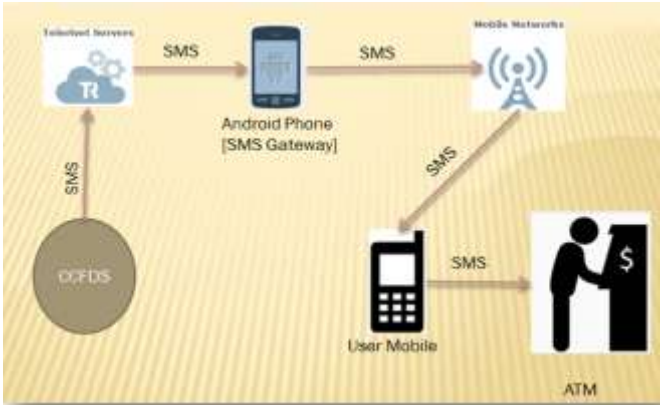

Figure 5: One-Time-Password

5. Results Analysis

The researchers used a financial dataset with 200 different transactions performed over a period of 6 months. The dataset was divided into two equal parts, that is, 100 entries for the training set and 100 for testing set.

Test Scenario for following account number; 11931000229, 11931000228 and 11931000227

Account Number	Test Case	Location	Day	Amount	Time	Exp Decision	Act. Decision
11931000229	1	N	N	N	N	¬S	¬S
	2	A	N	N	N	S	S
	3	N	N	A	N	S	S
	4	N	N	N	A	S	S
	5	N	A	N	N	S	S
11931000228	6	N	N	N	N	¬S	S
	7	A	N	N	N	S	S
	8	N	N	A	N	S	S
	9	N	N	N	A	S	S
	10	N	A	N	N	S	S
11931000227	11	N	N	N	N	¬S	¬S
	12	A	N	N	N	S	S
	13	N	N	A	N	S	S
	14	N	N	N	A	S	S
	15	N	A	N	N	S	S

Figure 6: Accounts test results

Key
S: Suspicious Transaction
¬S: Non-Suspicious Transaction
N: Normal Transaction
A: Abnormal Transaction

Figure 6 shows 15 transactions which performed in three different accounts and the results are recorded. For each account, there is one case where all the variables are normal **(N)** and four cases where time, amount, location and day variables have been tweaked. The application classified only one transaction as False Positive (**FT**) and there are no transactions classified as False Negative (**FN**). From the 15 transactions performed, the application only failed to correctly classify one transaction. Hence, the system scored 93.33% accuracy in classifying transactions. When the application was tested on a dataset with 100 entries and recorded **0.11612727247303815** as the Mean Square Error.

6. Conclusion

A cardholder's spending profile is susceptible to changes over time. These changes may be due to a change of residence, an increase or decrease in earnings of the cardholder. Identifying anomalies in this environment requires a system that analyzes the cardholder's profile. To address this, the researchers have adopted the HMM concept to generate a cardholder's profile based on the cardholder's past transactions. Hence, with this approach, the CFDS is able to adjust to changes in cardholder's profile when detecting anomalies

The proposed CFDS provides two – level security to the ATM. First, the cardholder is requested to provide a valid PIN to initiate a transaction. Second, the CFDS models the cardholder's profile based on previous transactions and compares it with the profile reflected in the on-going transaction. If anomalies are identified, the cardholder performing the transaction is requested to provide a valid token that would have sent to the mobile number associated with the account on which the transaction is performed. This way, security is ensured since it is very unlikely that cardholder may lost their card, PIN and mobile phone to the same person.

7. Limitations

a) Total time taken to complete a transaction
When anomalies are identified in the cardholder's profile for an on-going transaction, the system adds 60 seconds (assumptions) to the total time of transaction the cardholder would have taken. This is meant to provide room for the cardholder to confirm his/her identity by providing a valid token would have sent to the mobile phone. Although it appears to be inconvenient regarding time of service, the cost of inconveniencing the customer has less negative impact as compared to the cost of customers losing money to fraudsters.

b) Mobile phone
Confirming a transaction with token requires the cardholder have his/ her mobile phone ready. However, this is not always the case with many cardholders.

References

[1] Lucian, V., Matthew, W. & David, M., 2003. Defining Fraud: Issues for Organizations from an Information Systems Perspective. In *7th Pacific Asia Conference on Information Systems,*. Adelaide, 2003. Austria.
[2] Koponen, 2014. *E-COMMERCE, ELECTRONIC PAYMENTS*. [Online] Available at: HYPERLINK "http://home.ku.edu.tr/~daksen/mgis410/materials/E-Commerce_Electronic_Payments.pdf" http://home.ku.edu.tr/~daksen/mgis410/materials/E-Commerce_Electronic_Payments.pdf .
[3] Ali, M.., Budi, A., Martin, E. & Aad, v.M., 2017. Does The Online Card Payment Landscape Unwittingly Facilitate Fraud? *IEEE Security & Privacy*.

[4] Australia Cyber Security Centre, *2017*. [Online] Available at: HYPERLINK "https://www.asd.gov.au/publications/protect/Multi_Factor_Authentication.pdf" https://www.asd.gov.au/publications/protect/Multi_Factor_Authentication.pdf [Accessed 13 September 2017].

[5] Katharina, K., Heidelinde, H., Markus, H. & Edga, r.W., 2014. *Advanced Social Engineering Attacks*. [Online] SBA Research Available at: HYPERLINK "https://www.sba-research.org/wp-content/uploads/publications/jisa_revised.pdf" https://www.sba-research.org/wp-content/uploads/publications/jisa_revised.pdf [Accessed 13 September 2017].

[6] David, B., 2015. *5 Social Engineering Attacks to Watch Out For*. [Online] Available at: HYPERLINK "https://www.tripwire.com/state-of-security/security-awareness/5-social-engineering-attacks-to-watch-out-for/" https://www.tripwire.com/state-of-security/security-awareness/5-social-engineering-attacks-to-watch-out-for/ [Accessed 13 September 2017].

[7] Tatira, Z., 2017. *Cash crisis to continue*. [Online] Available at: HYPERLINK "https://www.newsday.co.zw/2017/06/cash-crisis-continue/" https://www.newsday.co.zw/2017/06/cash-crisis-continue/ [Accessed 13 September 2017].

[8] Kabweza, 2017. *Electronic money now 70% of all payments in Zimbabwe… and other central bank updates*. [Online] Available at: HYPERLINK "http://www.techzim.co.zw/2017/05/electronic-money-now-70-payments-zimbabwe-central-bank-updates/" http://www.techzim.co.zw/2017/05/electronic-money-now-70-payments-zimbabwe-central-bank-updates/ [Accessed 13 September 2017].

[9] Mazo, R. & Choga, F., 2015. The Impact of Electronic Technologies on Commercial Banks in Harare, Capital City of Zimbabwe (2009-2014). *The International Asian Research Journal*, 3(1), pp.5-10.

[10] Aihua, S., Rencheng, T. & Yaochen, D., 2007. Application of Classification Models on Credit Card Fraud Detection. *IEEE*.

[11] Kelli, G., 2017. *Identity theft, fraud cost consumers more than $16 billion*. [Online] Available at: HYPERLINK "https://www.cnbc.com/2017/02/01/consumers-lost-more-than-16b-to-fraud-and-identity-theft-last-year.html" https://www.cnbc.com/2017/02/01/consumers-lost-more-than-16b-to-fraud-and-identity-theft-last-year.html [Accessed 13 September 2017].

[12] Haydn, S., 2011. *Solving the $190 billion Annual Fraud Problem: More on Jumio*. [Online] Available at: HYPERLINK "https://www.forbes.com/sites/haydnshaughnessy/2011/03/24/solving-the-190-billion-annual-fraud-scam-more-on-jumio/" \l "6a74e29a390e" https://www.forbes.com/sites/haydnshaughnessy/2011/03/24/solving-the-190-billion-annual-fraud-scam-more-on-jumio/#6a74e29a390e [Accessed 13 September 2017].

[13] Kerry, C., 2016. *Credit Card Fraud in the U.S. Topped $8 Billion in 2015*. [Online] Available at: HYPERLINK "http://time.com/money/4544400/credit-card-fraud-us/" http://time.com/money/4544400/credit-card-fraud-us/ [Accessed 13 September 2017].

[14] Machakaire, T., 2014. *fbc-bank-tellers-up-for-500k-fraud*. [Online] Available at: https://www.dailynews.co.zw/articles/2014/01/31/fbc-bank-tellers-up-for-500k-fraud [Accessed 15 September 2017].

[15] Rupapa, T., 2015. *manager-siphons-182k-from-steward-bank*. [Online] Available at: http://www.herald.co.zw/manager-siphons-182k-from-steward-bank/ [Accessed 15 September 2017].

[16] Satvik, V., Surya, K.. & Naveen, K.P., 2013. Genetic algorithms for credit card fraud detection. In *International Conference on Education and Educational Technologies*. Uttar Pradesh, India, 2013.

[17] RamaKalyani & UmaDevi, 2012. Fraud Detection of Credit Card Payment System by Genetic Algorithm. *International Journal of Scientific & Engineering Research*, 3(7).

[18] Danie, l.J. & James, H.M., 2017. *Hidden Markov Model*. [Online] Available at: HYPERLINK "https://web.stanford.edu/~jurafsky/slp3/9.pdf" https://web.stanford.edu/~jurafsky/slp3/9.pdf [Accessed 13 September 2017].

[19] Dave, G., 2017. *Researchers are using Darwin's theories to evolve AI, so only the strongest algorithms survive*. [Online] Available at: HYPERLINK "https://qz.com/933695/researchers-are-using-darwins-theories-to-evolve-ai-so-only-the-strongest-algorithms-survive/" https://qz.com/933695/researchers-are-using-darwins-theories-to-evolve-ai-so-only-the-strongest-algorithms-survive/ [Accessed 13 September 2017].

[20] Sibi, Allwyn, J. & Siddarth, 2013. ANALYSIS OF DIFFERENT ACTIVATION FUNCTIONS USING BACK PROPAGATION NEURAL NETWORKS. *Journal of Theoretical and Applied Information Technology*, 47(3).

[21] Ming, L., 2008. *Introduction to Artificial Neural Networks*. [Online] Available at: HYPERLINK "http://cis.poly.edu/~mleung/CS6673/s09/introductionANN.pdf" http://cis.poly.edu/~mleung/CS6673/s09/introductionANN.pdf [Accessed 13 September 2017].

Author Profile

Elliot Mbunge finished Bsc in Information Technology with Chinhoyi University of Technology and Msc in Information Systems with Midlands State University in 2013 and 2016, respectively.

Ralph Makuyana, Nation Chirara and Antony Chingosho each finished Bsc in Information Technology with Chinhoyi University of Technology in 2016.