Credit Card Fraud Detection System in Commercial Sites

Akinbohun Folake, and Atanlogun Sunday Kolawole

***Abstract*—In modern retail market, electronic commerce has rapidly gained a lot of attention and also provides instantaneous transactions. In electronic commerce, credit card has become the most important means of payment due to fast development in information technology around the world. The objective of the paper is to develop a credit card fraud detection system in commercial sites. It is designed as a web based application in which transition state model was adopted for the research process. PHP (Hypertext Pre-Processor) is used for application development and MySQL to generate databases. The result shows that the system performance is performing to its task and therefore recommended to electronic commerce owners to ensure data integrity and security of their customers.**

***Index Terms*—Card; Commerce; Detection; Transaction.**

I. Introduction

Credit card is a means for buying and selling goods and services without having cash in hand [3]. It is a simple way of offering credit to a consumer automatically. A credit card is a plastic card that provides the cardholder electronic access to his/her bank account at a financial institution. Credit card can be used in two ways: physically and virtually. The Physical usage allows an individual to use the card for purchase in any store personally or physically while the virtual usage or online usage allows the card owner to use the card to pay for purchased item online over the internet by just entering the required card details. If an attacker gains access to all information about the card, they can gain access to the account which can result into a substantial financial loss.

The rapid growth of credit card use on the Internet has caused database security loses. Millions of accounts have been compromised [7].

Incidences of credit card fraud have resulted in huge financial losses as the fraudulent transactions are on the large value transactions. Out of 12 billion transactions made annually, approximately 10 million or one out of every 1200 transactions turned out to be fraudulent in 1999 [6]. In the decade to 2008, general credit card losses have been $0.07 or less per $100 of transactions [5]

As enormous growth of e-commerce over the internet, globalization is increased; credit card fraud is one of the biggest threats to commercial websites which can cause huge amount of loss in different countries as a result of credit card usage in an online transaction [1]

Published on November 1, 2018.

F. Akinbohun is with Department of Computer Science, Rufus Giwa Polytechnic, Owo, Ondo State, Nigeria (e-mail: folakeakinbohun@yahoo.com).

S. K. Atanlogun is with the Department of Mathematics and Statistics, Rufus Giwa Polytechnic, Owo, Ondo State, Nigeria. (e-mail: atanlogunkola@yahoo.com).

Considerable scandals that have been experienced in commercial banks with the use of credit cards have reduced the confidence the customers (cardholders) have in their banks, during the past five years or more.

These scandals have financially devastated banks' customers and severely harmed the reputation of some banks. It is in realization of this that various initiatives have put in place to enhance the detection of such fraud. A credit card fraud detection system looks for anomalous or malicious behavior in the pattern of activity of the cardholder

II. Related Work

A credit card fraud detection system in a commercial (e-commerce) websites is a system that monitors the activities of a cardholder on an e-commerce site for malicious activities or policy violations and ensures that any detected malicious suspicious activity is blocked before the fraudulent act.

Khan *et al*. [4] remarked that technology plays a vital role in improving the quality of services provided by the business units. One of the technologies which really brought information revolution in the society is internet technology and is rightly regarded as the third wave revolution after agricultural and industrial revolution. The cutting edge today is e-commerce.

Baton *et al.* [1] highlighted in their paperwork the physical characteristics of credit cards: The size of most credit card is 85.60mm*53.98{3.370in *2.125in} and rounded corners with a radius of 2.88-3.48mm conforming to the ISO/IEC 7810 ID-1standard, the same as debit cards.

Bhatla *et al* [2] highlighted in their paperwork the role of credit card issuing company, such as banks or credit unions, they enter into agreement with merchants for them to accept their credit cards. Merchants often advertise which card they accept by displaying acceptance marks, generally derived from logo's or this may be communicated in signage in the establishment or in a company material. The credit card issuer, issues a credit card to a customer at the time or after an account has been approved by the credit card provider, which need to be the same entity as the card issuer. The cardholder can then use it to make purchase at the merchant accepting that card. When purchase is made, the cardholder agrees to pay the card issuer. The cardholder indicates consent to pay by signing a receipt with a record of the card details and indicating the amount to be paid or by entering a Personal Identification Number (PIN).

Stephen [16] described that there are statistical and non-statistical approaches that are useful in credit card fraud detection. Unsupervised approaches for anomaly detection can prove extremely useful in credit card fraud detection. He further said that solid feature engineering is extremely

important for spotting credit card fraudsters. Principal Component Analysis (PCA) is also useful in feature engineering which allow viewing clusters of high dimensional customer behaviour to gain an understanding of the distribution of behaviour among different groups of customers.

Nuno et al., [15] described the development and deployment of a fraud detection system in a large e-tail merchant where they explored the combination of manual and automatic classification that gave insights into the complete development process and compared different machine learning methods. The work paper helped researchers and practitioners to design and implement data mining based systems for fraud detection or similar problems.

Gangeshwer [14] reviewed the conceptual knowledge of search engine marketing (SEM) or e-commerce, literatures, current and future aspects of e-commerce in Indian context and focused on the top motivator factors of shopping online.

John et al [13] compared machine learning techniques on credit card fraud detection. The research investigated the performance of naïve bayes, k-nearest neighbor and logistic regression on highly skewed credit card fraud data. Dataset of credit card transactions was sourced from European cardholders containing 284,807 transactions. A hybrid technique of under-sampling and oversampling were carried out on the skewed data. The work was implemented in Python.

Masoumeh and Pourya [12] worked on the application of Credit Card Fraud Detection using Bagging Ensemble Classifier. They trained various data mining techniques used in credit card fraud detection and evaluate each methodology based on certain design criteria. After several trial and comparisons; they introduced the bagging classifier based on decision three, as the best classifier to construct the fraud detection model.

Alex et al. [11] proposed a customized classification algorithm for credit card fraud detection. They presented a customized Bayesian Network Classifier (BNC) algorithm for a real credit card fraud detection problem. They created Fraud-BNC that was automatically performed by a Hyper-Heuristic Evolutionary Algorithm (HHEA), which organized the knowledge about the BNC algorithm into taxonomy and searched for the best combination of these components for a given dataset.

Delamaire et al. [10] reviewed credit card fraud and detection techniques. The main aims are to identify the different types of credit card fraud and to review alternative techniques that have been used in fraud detection. Different publications on credit card fraud detection were compared and analysed. The significance of the application of the techniques reviewed was in the minimization of credit card fraud. Yet there were still ethical issues when genuine credit card customers were misclassified as fraudulent.

Dheepa and Dhanapal [8] analysed methods of credit card fraud detection. They presented three methods to detect fraud. The main task was to explore different views of the same problem and see what can be learned from the application of each different technique. Different techniques were used such as Clustering model, Guassian Mixture model and Bayesian network. Clustering model was used to classify the legal and fraudulent transaction using data clusterization of regions of parameter value and Gaussian Mixture model was used to model the probability density of credit card user's past behavior so that the probability of current behavior can be calculated to detect any abnormalities from the past behavior. Lastly, Bayesian networks were used to describe the statistics of a particular user and the statistics of different fraud scenarios.

Dahee and Kyungho [9] worked on a survey and Implementation of financial fraud detection under IoT environment. They described financial fraud under IoT environment as the fast-growing issue through the emergence of smartphone and online transition services. They surveyed financial fraud methods using machine learning and deep learning methodology from 2016 to 2018. Their approach proposed the overall process of detecting financial fraud based on machine learning and compared with artificial neural networks approach to detect fraud and process large amounts of financial data. The final model was validated by the actual financial transaction data occurring in Korea, 2015.

III. METHODOLOGY

Due to fraud that costs consumers and the financial company billions of dollars annually; and fraudsters continuously try to find new rules and tactics to commit illegal actions, therefore there is need to design fraud detection systems for banks and financial institution to minimize their losses.

The aim of this study is to detect fraudulent operations on credit card at the point of transaction on an e-commerce site by the card holder's spending habit using transition state model. This study considers the spending routines of the cardholder. In this study, transactions of the credit card processing series are modeled by the stochastic procedure. The system consists of the transaction section, the detection section and the monitoring section used by the card issuing bank. To map the bank card transaction processing operation in terms of transaction state model, the past numbers "n" of transactions of the cardholder is categorized into three categories the low, medium and high.

To achieve the stated objectives, transition state model was adopted. The system takes the state of the past transactions which could be low, medium or high, compare it with the new transaction under processing, if the previous state match with the new state, transaction is allowed; otherwise, the transaction process is treated as fraudulent.

The design was a web-based application and implemented on a database using MYSQL (My Structured Query Language). For the front-end of the application Hypertext Mark-up Language (HTML) and Cascading Style Sheet (CSS) are used while Hypertext Pre-processor is used to handle the server-side of the design. This work is done as a result to solve the problems usually encountered in most companies. The system architecture is presented in Fig. 1.

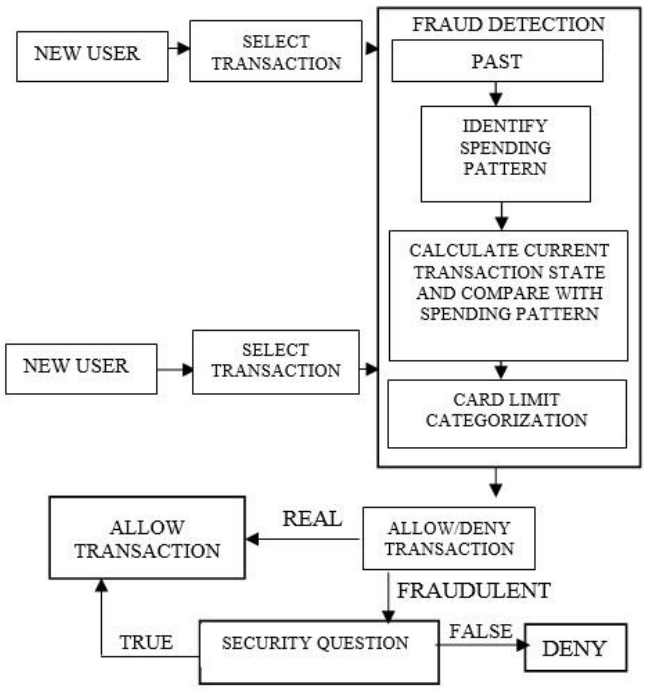

Fig. 1. Architectural Framework of Credit Card Fraud Detection System (CCFDS)

From the above architecture, the user/cardholder logs on to the e-commerce site, performs his/her transaction with their card, at the verification phase the user tries to check out and pay for the goods purchased, the profile creation of the user comes in, if the user is new, in order to determine the state of the transaction of the new user, it does the categorization using the card limit of the new users, otherwise, the categorization is done using the past transactions.

In order for the transaction to be carried out by the new user to be successful, the cardholder is required to answer some security question i.e. what's the name of your favorite food? what is your mother maiden name? etc. The system continually observes the cardholders spending habit, if the state changes, it takes the change of state to be fraudulent, then request for the security information to be answered.

A. Design Phase

Once a transaction process has been initiated, the system fetches the past transactions of the user and performs probabilistic calculations on it using the transitional state model given above. The spending habit of the user is determined from the categorization of the past transactions. The state of the past transactions is compared with the new transactions for fraudulent detection, if the previous state matches the new state, the transaction is allowed, otherwise, the transaction is denied.

B. Transition State Model (TSM)

Transition state model is assumed to be a statistical model which deals with probability distribution. Transitions among the states are governed by a set of probabilities according to the probability distribution. It is only the outcome, not the states that is visible to an external observer. It is a solution for addressing detection of fraud transaction through credit card.

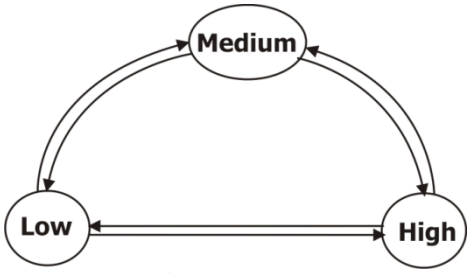

Fig. 2. Transition State of the Credit Card Fraud Detection System (CCFDS)

C. Algorithm for CCFDS

The algorithm for transition states is as shown below:

The categorization (c) Transaction State (Cts) contains three states that categorize into low (L), medium (M) and high (H) as presented category below:

$$\text{category} \begin{cases} L = N_t < 20\% \text{ of } T_{TOTAL} \\ M = 20\% \text{ of } T_{TOTAL} \geq N_t < 70\% \text{ of } T_{TOTAL} \\ H = 70\% \text{ of } T_{TOTAL} \geq N_t \end{cases}$$

Fraud is monitored using three basic factors such as the Current Transaction State (Cts), Last Transaction State (Lts) and Security Questions (Sq) where Lts = Cts = c. Transaction State (Ts) is directly proportional to Security questions as stated in Equation 1

$$Ts \alpha Sq \quad (1)$$

The Ts could be in Current transaction state (Cts) and last transaction state (Lts). Both Cts and Lts could be in any categorization either low, medium or high. Hence Cts and Lts are checked as follows in Equation 2

$$Cts_{(L, M, H)} \alpha Lts_{(L, M, H)} \quad (2)$$

In each transaction state, it becomes:

```
IF Cts == Lts
        Ts = 1;
IF Cts !=  Lts
        Sq == 1
        Ts = 1
IF Cts !=  Lts
        Sq == 0
        Ts = 0;1
Where
        Ts represents Transaction Status
        1 represents True (Allowed)
        0 represents False (Disallowed)
        α represents directly proportional
        == means equal to
        ! = means not equal to
```

D. Transaction Processing

In the transaction processes are presented below, the customer:

1. login
2. scan through the e-commerce website, add product to cart
3. supplies credit card information

4. If valid, transition state categorization/verification is done to determine the customer spending habit.
5. If transaction id found not to be fraudulent, access is allowed
6. If transaction is detected to be fraudulent, security questions are provided
7. If answers to security questions provided are right, access is allowed.
8. If not, access is denied.

From the above highlighted transaction process, username and password as a form of encryption is used for the user validation. The user has the ability to add items to cart which can later be checked out and subjected to further processing.

On the payment portal as seen in Fig. 5, the user is requested to supply a card detail which is validated as well. During the process, transition state model was used to determine the spending pattern of the user. If there is change in the user's state, the system treats the card holder and the current transaction as fraud where security questions are used for verification. If correct answers to the given security questions are correct, such transaction is allowed, otherwise, the current transaction is denied and the card is subjected to blockage.

IV. System (CCFDS) Output

Following the procedures in Algorithm for the dsign of CCFDS, the product interfaces are produced. Fig. 3 contains various categories of items (produts) to shop and their prices. The user click Add to CART to indicate the products to purchase.

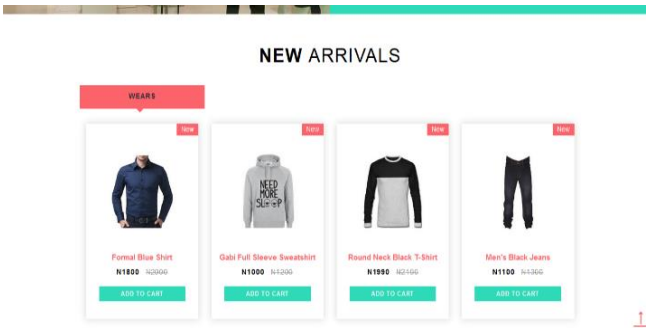

Fig. 3. Product

Fig. 4 is another interface which consists of the items/products, prices and quantity of what to purchase. The grand total is calculated.

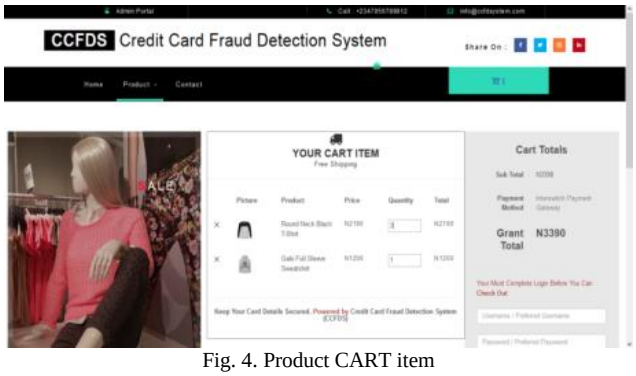

Fig. 4. Product CART item

Fig. 5 is the Admin Dashboard where the dashboard displays product management, customer management ans system setting. The number of total products, number of total orders,and numbers of customers are displayed. The board contains Ordering Tablefor products, price, order id and dellivery status.

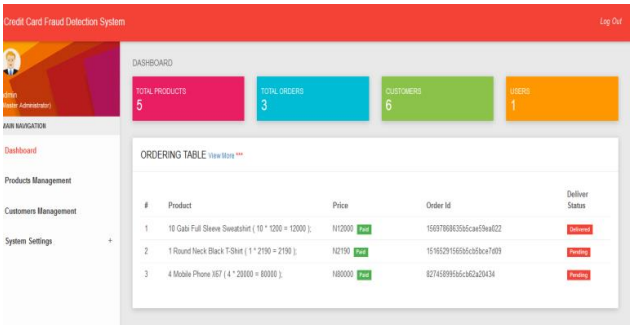

Fig. 5. Admin Dashboard

Fig. 6 is a module for payment where Automated Teller Machine (ATM) cards are registered and validated. It contains templates for registered cards, block cards and unblocked cards.

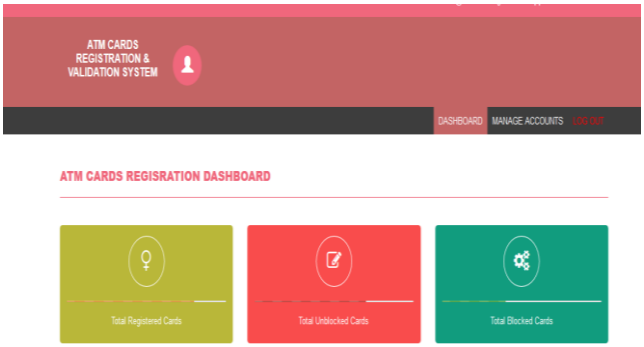

Fig. 6. Template for payment

References

[1] R.J. Baton and D. J. Hand (2002). A review on statistical fraud detection: statistical science. *International Journal of Science and Technology*. Volume 17, issue I, pp 15.

[2] T.P. Bhatla, V. Prabhu and A. Dua, (2003). Understanding credit card frauds: a review on card Business.Pp 20.

[3] D. Kayong, Z. Ru and G. Hong (2012). Analysis and study of detection of credit card fraud in E-commerce. Vol.13 pg 12-17

[4] M. S. Khan and S. S. Mahaptra (2011). Service quality evaluation in internet banking website quality in India: A webqual approach great lakes herald pg 40-58

[5] Paterson, Ken, Credit card issuer fraud management, report highlights. Mercator Advisory Group. Archived from the original *(PDF)* December 2008

[6] Hassibi, Khosrow, *Detection payment card fraud with neural networks* in book. Business Applications of neural networks, Singapore-New Jersey-London-Hong Kong: World Scientific, 2000, pp. 141–158.

[7] Court filings double estimate of TJX breach 2007

[8] V. Dheepa and R. Dhanapal R. (2009.) Analysis of Credit Card Fraud Detection Methods

[9] Dahee Choi and Kyungho Lee (2018). An Artificial Intelligence Approach to Financial Fraud Detection under IoT Environment: A Survey and Implementation.

[10] L. Delamaire, Hussein A. Abdou and John Pointon (2009). Credit card fraud and detection techniques: A review

[11] G. C. Alex, de Sa, C. M. Adriaono, Pereira Gisele L., Pappa (2018**)** A customized classification algorithm for credit card fraud detection. *Engineering Applications of Artificial Intelligence*. Published by Elsevier. Volume 72, pages 21-29

[12] Masoumeh Zareapoor and Pourya Shamsolmoali (2015). Application of Credit Card Fraud Detection: Based on Bagging Ensemble Classifier. *International Conference on Artificial Intelligent Computing, Communication and Convergence*. Procedia Computer Science. Volume 48, pages 679-685

[13] John O Awoyemi, Adebayo O. Adetunmbi and Samuel A. Oluwadare (2017). Credit card fraud detection using machine learning techniques: A comparative analysis. International Conference on Computing Network and Informatics (ICCNI)

[14] D. K. Gangeshwer (2005). E-Commerce or Internet Marketing: A Business Review from Indian Context. *International Journal of u- and e- Service, Science and Technology* Vol.6, No.6 (2013), pp.187-194. http://dx.doi.org/10.14257/ijunesst.2013.6.6.17

[15] Nuno Carneiro, Goncalo Figueira and MiguelCosta (2017). A data mining based system for credit-card fraud detection in e-tail. *Decision Support Systems*. Volume 95 March 2017, Pages 91-101

[16] Stephen Whitworth. What kind of statistical methods are used in credit card fraud detection and anti-money laundering. February 23, 2016

Akinbohun Folake hails from Ondo State in Nigeria. She bags Master of Technology in Computer Science from Federal University of Nigeria in 2012. Her areas of specialization are Data Science and e-commerce. She has been working in the Department of Computer Science, Rufus Giwa Polytechnic, Owo, Ondo State for 14 years. She is a member of Nigeria Computer Society (NCS). Mrs. Akinbohun Folake was a supervisor for Computer Program at her work place from 2010 to 2017.

Atanlogun Sunday Kolawole is from Akure, Ondo State, Nigeria. He possesses Master of Science (M. Sc) in Mathematics and Statistics.

He works in the Department of Mathematics and Statistics, Rufus Giwa Polytechnic, Owo, Ondo State. Mr. Atanlogun serves as a member in Accreditation Committee. He is a member of Nigeria Statistical Society.