International Journal of Electrical Electronics & Computer Science Engineering
Volume 6, Issue 6 (December, 2019) | E-ISSN : 2348-2273 | P-ISSN : 2454-1222
Available Online at www.ijeecse.com

An Enhanced Credit Card Transaction for Outlier Fraud Detection System Using Artificial Neural Network (ANNs)

J. B. Ochen[1], L. N. Onyejegbu[2], F. E. Onuodu[3]
[1-3]Department of Computer Science, University of Port Harcourt, Port Harcourt, Rivers State, Nigeria
[1]jeanebukie@gmail.com, [2]nneka2k@yahoo.com, [3]gonuodu@gmail.com

Abstract: ***Credit card fraud (CCF) is a recurrent problem all over the world. Some countries, despite having a low or average use of credit card, have a high percentage of credit card fraud recorded. The use of credit card that is (cashless) economy is important to any growing nation. Outlier detection aims at finding patterns in data that do not conform to expected behavior in the credit card transaction; it also has extensive use in a wide variety of applications such as military surveillance for enemy activities, intrusion detection in cyber security, fraud detection for credit cards, insurance or health care and fault detection in safety critical systems. In this work, we developed an enhanced credit card transaction for outlier fraud detection system using an artificial neural network algorithm called cortical learning algorithm and customer self-strip detection (OTP, Account Number and BVN) for detecting fraud from the user (the customers) perspective. In the admin column, it converts the highly populated data to a sparse polar representation. Support Vector Machine was used to train active data on the customers' column which is our area of concentration. Structured System Analysis and Design Methodology (SSADM) and PHP programming language are used in implementing .MySQL and Simplified unified database are used for NUBAN for every report made from the customer. The parameters for our result performance achieved an overall performance rate of 95% when compared with the most recent Outlier Fraud Detection System for Flight Reservation Booking. The parameters for the comparison included Time Complexity (TC), Life-Cycle Assessment (LCA), Benchmarking (B), Multi-Criteria Decision Making (MCDM), Risk Assessment (RA), Cost Benefit Analysis (CBA) and Speed (S) presented as TC, LCA, B, MCDM, RA, CBA, S = 21, 15, 7, 22, 8, 10, 12 respectively.***

Keyword: Credit Card Fraud, Support Vector Machine, Intrusion Detection.

I. INTRODUCTION

In recent times, Outlier detection aims to find patterns in data that do not conform to expected behavior. It has extensive use in a wide variety of applications such as military surveillance for enemy activities, intrusion detection in cyber security, fraud detection for credit cards, insurance or health care and fault detection in safety critical systems. Their importance in data is due to the fact that they can translate into actionable information in a wide variety of applications. An anomalous traffic pattern in a computer network could mean that a hacked computer is sending out sensitive data to an unauthorized destination[1].

An abnormal MRI image may indicate presence of malignant tumors[2] Outliers in credit card transaction data could indicate credit card or identity theft[3] or abnormal readings from a space craft sensor could signify a fault in some component of the space craft[4].

With the development of information technologies, the number of databases, as well as their dimension and complexity, grow rapidly, resulting in the necessity of automated analysis of great amount of heterogeneous structured information. For this purposes, data mining systems are used. The goal of these systems is to reveal hidden dependences in databases[5]. The analysis results are then used for making a decision by a human or program, such that the quality of the decision made evidently depends on the quality of the data mining.

One of the basic problems of data mining (along with classification, prediction, clustering, and association rules mining problems) is that of the outlier detection[6][7]. The outlier detection is searching for objects in the database that do not obey laws valid for the major part of the data. The identification of an object as an outlier is affected by various factors, many of which are of interest for practical applications. For example, an unusual flow of network packages, revealed by analyzing the system log, may be classified as an outlier, because it may be a virus attack or an attempt of an intrusion. Another example is automatic systems for preventing fraudulent use of credit cards. These systems detect unusual transactions and may block such transactions on earlier stages, preventing, thus, large losses. The detection of an object–outlier may be an evidence that there appeared new tendencies in data.

For example, a data mining system can detect changes in the market situation earlier than a human expert. The outlier detection problem is similar to the classification problem. A specific feature of the former, however, is that the great majority of the database objects being analyzed are not outliers. Moreover, in many cases, it is not a priori known what objects are outliers.

In this work, we consider basic approaches used currently in data mining systems for solving the outlier detection problem. Methods based on kernel functions are considered in more detail, and their basic advantages and disadvantages are discussed. A new algorithm for detecting outliers is suggested, which possesses a number of advantages compared to the existing methods. It makes use of kernel functions and relies on methods of fuzzy set theory. The performance of the suggested algorithm is examined by the example of the

applied problem of anomaly detection, which arises in computer protection systems, the so-called intrusion detection systems [8].

Since then several research communities have developed a variety of outlier detection techniques with many of these specifically meant for certain applications and others being generic in nature. With this exercise, we hope to get a better understanding of the different directions of research on outlier analysis and think of applying techniques in different areas to our areas of interest of crime detection and counter terrorism, even if they were not intended, to begin with.

Credit card fraud (CCF) is a recurrent problem all over the world that some countries, despite having a low or average use of credit card, have a high percentage of credit card fraud recorded. Credit card fraud can happen several ways. Your card could be lost or stolen and used to purchase goods and services. A criminal could obtain your card number and expiry date and use this information to buy merchandise by phone or over the Internet. Or criminals could tamper with payment terminals at retailers to obtain your card information and create a counterfeit credit card.

Contrary to popular belief, merchants are far more at risk from credit card fraud than the cardholders. While consumers may face trouble trying to get a fraudulent transaction reversed, merchants lose the cost of the product sold, pay chargeback fees, and fear from the risk of having their merchant account closed. Increasingly, the *card not* present scenario, such as shopping on the internet poses a greater threat as the merchant (the web site) is no longer protected with advantages of physical verification such as signature check, photo identification, etc. In fact, it is almost impossible to perform any of the 'physical world' checks necessary to detect who is at the other end of the transaction. This makes the internet extremely attractive to fraud perpetrators. According to a recent survey, the rate at which internet fraud occurs is 12 to 15 times higher than 'physical world' fraud. However, recent technical developments are showing some promise to check fraud in the card not present scenario.

With all the negative impacts of fraudulent credit card activities – financial and product losses, fines, loss of reputation, etc, and technological advancements in perpetrating fraud – it's easy for merchants to feel victimized and helpless. However, technological advancements in preventing fraud have started showing some promise to combat fraud. Acquirers and Issuers are creating innovative solutions to bring down on fraudulent transactions and lower merchant chargeback rates.

One of the main challenges with fraud prevention is the long time lag between the time a fraudulent transaction occurs and the time when it gets detected, i.e., the cardholder initiates a chargeback. Analysis shows that the average lag between the transaction date and the chargeback notification could be as high as 72 days. This means that, if no fraud prevention is in place, one or more fraudsters could easily generate significant damage to a business before the affected stakeholders even realize the problem. Hence it is expected that proactive measures are put in place to curb Credit Card Fraud before it becomes uncontrollable in our nation.

II. RELATED WORK

[9] proposed a fraud detection system for credit card using a three-layer approach of feed forward neural network. The system was trained on a sample of labeled data that included all the activities on the account over a period of two months. Various kinds of fraud data were used to train the neural network. After the training, it recorded significant success in detecting fraudulent transactions than the earlier rule-based fraud detection systems used. However, the system required long training time.

[3] proposed a database mining technique to design a fraud detection system for credit cards using approach called CARDWATCH, the system was based on a neural network learning section and provided interface to a variety of commercial databases. The test results obtained from the detection model indicated high fraud detection rate. CARDWATCH exhibited high processing speed and great accuracy in fraud detection but has a shortcoming of requiring one network to one customer.

[10] proposed a clustering model, a similarity measure for estimating the degree of similarity between two symbolic patterns using K-mutual nearest neighborhood and mutual similarity is employed. The model uses tow layer clustering strategy. In the first layer, a similarity proximity matrix for symbolic pattern based on the proposed similarity measure is obtained. A position matrix is created from the similarity proximity matrix based on the similarity rank of pattern. The K-mutually nearest neighbor's algorithm is applied on the position matrix to obtain clusters of patterns. The proposed clustering model is based on a two layer clustering strategy. In the first layer, a similarity proximity matrix for symbolic patterns based on the proposed similarity measure is obtained. A position matrix based on the similarity proximity matrix based on the similarity rank of pattern. The K-mutually nearest neighbors' algorithm is applied on the position matrix to obtain clusters of patterns.

[11] published an article on digital signature that uses keys for files encrypted with the Public key can only be decrypted by the holder of the Private Key. Also, the difficulty in factoring out these keys makes RSA secured.

[12] stated that the biometric system is the absolute political weapon of our era" and a form of "soft

control." Two decades ago, biometric systems have entered the national market, and unclear the outline between legislative arms and private company control.

[13] pointed out the phrase "biometric authentication is perhaps more appropriate than biometrics since the latter has been historically used in the field of statistics to refer to the analysis of biological (particularly medical) data."

[14] Firmly speaking, accent is as well a physiological feature since each person has dissimilar vocal tract, however, voice identification are grouped as behavioral as it is influenced through a person's temper. Biometric voice identification are broken up and separated from speech identification as well as the last being considered with precise recognition of speech content instead of detection or identification of the individual talking.

[15] Proposed Biometric Identification Systems traits are physical, behavioral or adhered human characteristics, which have been derived from the way human beings normally distinguish their peers (e.g. height, gender, hair color)". They are applied to harmonize the uniqueness information given by the main biometric identifier. Though flexible biometric features require the individuality and durability to identify a person exclusively and dependably, and could be simply faked, they give a few facts concerning the end users personality which can be useful. That is, even though they are incapable of individualizing an issue, they are helpful in characterizing individuals. Two major ethical subjects are discussed through flexible biometrics.

[16] gave the subsequent definition concerning data as; "A graphic or textual representation of facts concepts, numbers, letters, symbols or instructions suitable for communication, interpretation or processing". Data are the essential part of information which are used to express things, thoughts, circumstances or conditions.

[17] applied two machine learning techniques; artificial neural networks (ANN) and Bayesian belief networks (BNN) in detecting credit card fraud. The work looked at the features of a new transaction to classify if the transaction is genuine or fraudulent. The STAGE approach (which is an instance of global optimization) was used in learning the topology of the BNN. Primary data was obtained by Serge Waterschoot at Europay International (EPI). The Receiver Operating Curve (ROC) was used to measure the performance of both the ANN and BNN systems. The ROC combined the information of true positive and false positive in a single graph, the true positive is plotted on the y-axis and false positive on the x-axis. The resulted graph showed that accuracy of predictions made depends on how much the system had learned. The ROC graph showed that BNN yields better results than ANN when applied to CCF detection, and the learning time in BNN is very short as compared to ANN, however, the CCF detection process is faster with ANN.

[18] put forward a new model for CCF detection using Artificial Immune Systems (AIS) named AIS-based Fraud Detection Model (AFDM) and the model was implemented on a cloud-base file system (cloud computing). The work extended the previous work done by Watkins et. al, 2004 by introducing distributed storage to the artificial immune recognition system, thereby allowing training phase to be done in a parallel manner hence reducing training time. An increase of fraud detection by 25%, reduced cost by 85% and decrease system response time up to 40% as compared to the base algorithm AIRS (Artificial Immune Recognition System) was recorded.

[19] mentioned that text classification is very necessary for the analysis and management of text as the availability of online text is increasing rapidly. According to them, text is not costly, but information, in the form of knowing what classes a text belongs to, is costly. In their paper, they used association rule mining method to get feature set from pre-classified text documents and derived features for final classification using Naïve Bayes classifier.

Chandrahas, et al (2017): [20] Credit card fraud Identification Using Artificial Neural Networks using three learning methods i.e. Gradient descent, Bayesian Regularization and LM technique. All the learning techniques are applied on same network and same configuration but we found different accuracy i.e. 98.74%, 98.63% and 95.57% using BR, GDA and LM techniques respectively on German (Statlog) credit dataset and 99.01%, 96.28% and 93.86% using BR, GDA and LM respectively on Australian credit dataset . Now from above experiment it is clear that the accuracy of result increased when network is trained by Bayesian Regularization Technique on both datasets i.e. German (Statlog) credit and Australian credit dataset. It is also observed that when sample size is increased then the performance of BR technique is also increased while performance of GDA and LM is decreased. Performance of BR technique is better than other two technique i.e. GDA and LM for larger size dataset. Therefore Bayesian Regularization Technique is better approach for training the multi-layer feed forward back propagation neural network for credit card fraud identification system. Availability of the real world dataset is the key challenge for credit card fraud identification system because financial institutions don't allow sharing the historical data of their customers due to privacy policy.

[21] worked on towards scalable learning with non-unified class and cost distribution: A case study in credit card fraud detection. They worked with very large database with skewed class distribution and non-uniform cost per error are not uncommon in real world data mining task. A multi-classifier metal- learning

approach was devised to address these three issues. Empirical results from a credit card fraud detection task indicate that the approach can significantly reduce loss due to illegitimate transaction.

[22] Detected credit card fraud by decision trees and support vector machine and classification of models based on decision trees and support vector machines (SVM) developing application on credit card fraud detection problem. The study was one of the firsts to compare the performance of SVM and decision tree methods in credit card fraud detection with a real data set.

[23] worked on a novel Machine Learning Approach to Credit Card Fraud Detection. The use of credit cards is of paramount importance in improving the economic strength of any nation, however, fraudulent activities associated with it is of great concern. When fraud occurs on credit cards, the negative impact is huge as the financial loss experienced cuts across all the parties involved. Their work provides a proactive measure at detecting fraudulent activities regarding the credit card. A novel approach in machine learning known as the cortical learning algorithm was adopted to build the credit card fraud. detection model. The algorithm worked on the credit card data obtained from the UCI Repository, it converted the highly populated data to a sparse representation, and then used its learning columns to learn spatial and temporal patterns. The object oriented analysis and design methodology was used in the design of the system which was implemented with JAVA programming language. The simulation was carried out with MATLAB programming language. The resulting model performed online learning and recorded higher percentage accuracy of 91% and beyond in detecting fraudulent transactions as compared to the Neural Network model that recorded 89.6%, hence, cases of misclassification was reduced to the barest minimum and efficiency of fraud detection was increased but lacked customer involvement in fraud detection.

III. MATERIALS AND METHODS

A.1. Analysis of the Existing System:

The use of credit card is rising day by day as the e-commerce is also increasing. The problem that happens with this is that fraud using credit card is increasing. It is a recurrent problem in almost all countries. But the trend seen is that countries with more credit card transactions are having less credit card fraud on the other hand countries with average credit card transactions are having high rate of credit card fraud. So in order to avoid this proactive methods are needed. In this a novel machine learning algorithm called cortical algorithm is used. It is the learning algorithm of hierarchical temporal memory and is inspired by the neo cortex of the brain.

This is a new approach for prediction and anomaly detection. It works on data obtained from UCI repository. The methodology is that it converts highly populated data into sparse representations and uses learning columns to learn spatial and temporal patterns. It mainly follows three steps in analyzing and predicting data from the streaming input.

The steps included are

(i) A sparse representation of the input is initially formed.

(ii) A representation is formed based on the previous input.

(iii) Finally a prediction is made based on previous step.

The system architecture is described in the figure 3.1 includes a user interface, Duration, Learning columns and a dataset. The duration and learning columns are used for analyzing the data and it is compared with the credit card data set which is obtained from the UCI repository. After analyzing and comparing the final step is predicting whether the transaction is fraudulent or not. This study provides an effective way to detect credit card fraud transactions.

A.2. Algorithm Used in the Existing System:

The existing system used cortical algorithm in detecting fraudulent act on credit cards used in the banking section. The algorithm is analyzed as follow:

(i) Start with an input consisting of a fixed number of bits. These bits might represent sensory data or they might come from another region lower in the hierarchy.

(ii) Assign a fixed number of columns to the region receiving this input. Each column has an associated dendrite segment. Each dendrite segment has a set of potential synapses representing a subset of the input bits. Each potential synapse has a permanence value. Based on their permanence values, some of the potential synapses will be valid.

(iii) For any given input, determine how many valid synapses on each column are connected to active input bits.

(iv) The number of active synapses is multiplied by a "boosting" factor which is dynamically determined by how often a column is active relative to its neighbors.

(v) The columns with the highest activations after boosting disable all but a fixed percentage of the columns within an inhibition radius. The inhibition radius is itself dynamically determined by the spread (or "fan-out") of input bits. There is now a sparse set of active columns.

A.3. Advantages of the Existing System:

International Journal of Electrical Electronics & Computer Science Engineering
Volume 6, Issue 6 (December, 2019) | E-ISSN : 2348-2273 | P-ISSN : 2454-1222
Available Online at www.ijeecse.com

(i) It works on data obtained from UCI repository which make the system less complex.

(ii) Very flexible for users.

(iii) Very effective on high dimensional data.

A.4. Disadvantages of the Existing System:

(i) Users are not involved in the fraud in the credit card fraud detection.

(ii) Lack of transparency of results.

(iii) Poor interoperability.

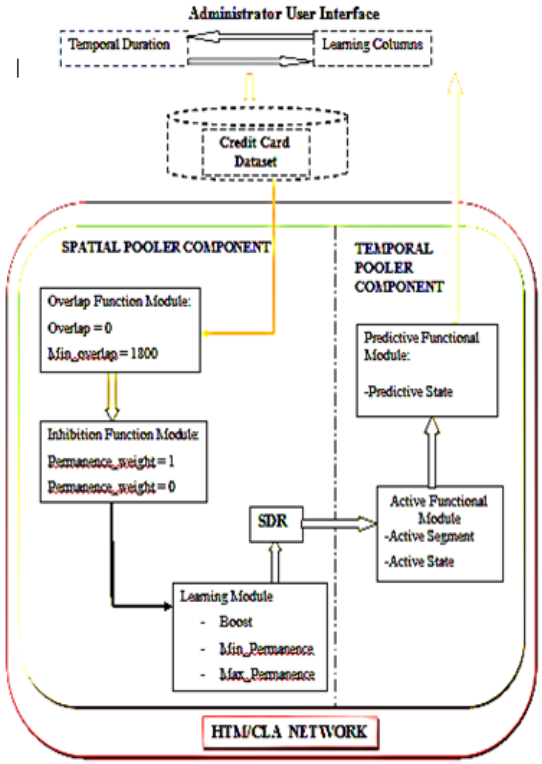

Fig. 1. Existing System Architecture

B. Proposed System:

We utilize the disadvantage of the existing system by profiling an adequate solution to it by allowing users to be involved in the fraud detection and blockage of the credit card transaction by initiating an OTP SMS to the system that will authenticate and validate ownership of the credit card which will increase the security of credit card usage.

In this evidence, the proposed credit card fraud detection system is based on the use of SVM and Neural Network: SVM Can classify both linear and nonlinear data Neural Network , Can classify patterns even if not trained data and Efficient to handle noisy data) rule based filter, Dempster Shafer adder, transaction history database and Bayesian learner. In rule base the suspicion level of each incoming transaction is determined. Dumpster Shafer is used to combine multiple such evidences and an initial belief is computed. Based on this belief the transactions are classified as normal, abnormal or suspicious. The incoming transactions are initially handled by the rule base using probability values.

After this the values are combined using Dumpster Shafer Adder. If the transaction is declared as fraudulent then it is handled by the card holder. If suppose the transaction is suspicious then it is fed in the suspicious table The score of transaction is updated in the database with the help of Bayesian classification. This architecture is flexible such that new kinds of fraud can be handled easily. With the help of Bayesian learner the system can dynamically adapt to the changing needs.

B.1. Analysis of the Proposed System:

In fig. 2, the proposed system is sub-divided into admin section and customer section. The admin section stores all the historical data, features and the methods at which all customer information are stored in the big database awaiting the same set of data form the online section

The customers section serves as a platform to enable blockage of credit card in case of fraudulent transaction. Here the information from the historical data in admin section is compared using Support Vector machine and Neural Network to validate the incoming information produce from the real owner of such card. In addition to these, the transaction carried out after the algorithm has done its comparison is subdivided into user transaction which is the legitimate transaction and fraudulent transaction which is the illegal transaction. The analyzed transaction can now be nullified if the transaction is not genuine.

B.2. Algorithm Used for Proposed System:

The proposed system used Artificial Neural Network (ANN) enhanced by Support Vector Machine (SVM) in detecting fraudulent transaction on credit card in the banking sector. The algorithm is analyzed as follows:

(i) Establish authentication for Self-care (using account number and password sent Via SMS during pre-registration) or Admin Login (Goto7)

(ii) Initiate pre-establish authentication parameters dataset with a switch mode to 3 (2-way) or 6 (None).

(iii) Preparation Step of Shared Secrets: generation of Authentication alpha Numeric pass code to identify preset dataset for onward transmission request by a customer.

(iv) SMS-Gateway Transmission: the shared secrets are been wrapper by URL-Encode data encryption system through designated registered SIDN over the Mobile network subsystem.

(v) Verifying and Validating Transmitted Shared Secrets: shared secrets notification are sent to mobile workstation of the SIDN verifier algorithm calculate the downlink OTP to prepared

International Journal of Electrical Electronics & Computer Science Engineering
Volume 6, Issue 6 (December, 2019) | E-ISSN : 2348-2273 | P-ISSN : 2454-1222
Available Online at www.ijeecse.com

stored shared secrets for match. If OTP match accepted then block process operation succeeded else fail OTP match will result to 2 again.

(vi) None 2way Authentication: on verified BVN code entry, block process operation succeeded else goto 2.

(vii) Admin operation: preregistration of customer and user login details sent via SMS to enable 2.

(viii) Simulated Transaction Operation: customer transaction logs are simulated for Deposit and withdrawal banking operation if customer account not block due to fraud detection.

(ix) View records: admin preview of all dataset of customer and transaction log.

(x) Unblock Status: process of step 2 to step 6 if succeeded, the admin can unblock customer status via update on pre-dataset else goto 1.

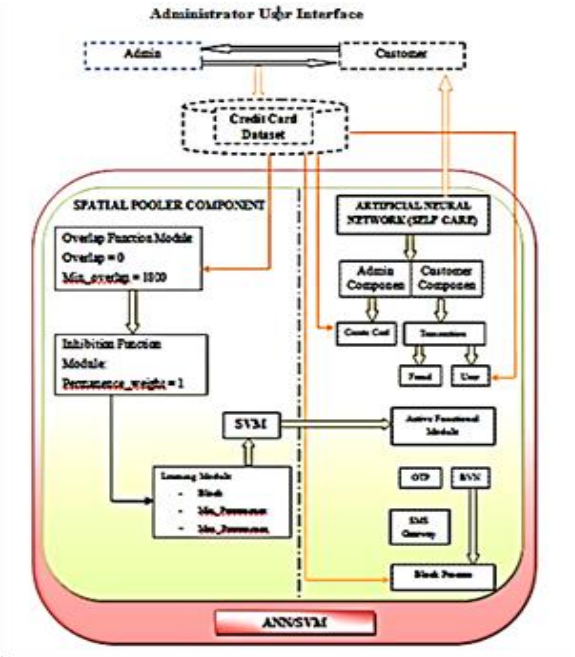

Fig. 2. Architecture of the Proposed System

B.3. Advantages of the Proposed System:

(i) Users friendly and easier in detecting fraud in banking sector.

(ii) The model in minimizing the total financial loss. The measure used is Saved Loss Rate (SLR) which is the saved percentage of the potential financial loss that is the sum of the available usable limits of the cards from which fraudulent transactions are committed.

B.4. UML Use Case and Class Diagrams of the Proposed System:

The use case diagram of the proposed system shows all the actors that must play their respective role (designated as use cases) in order for the proposed system to function according to its standard design specifications. A use case is an activity, an operation or function which an actor of the proposed system will have to perform within its designated class or sub-system. The fig. 3 presents a use case diagram of the proposed system. It shows a pictorial description of how the system's major actors interact with the system. The system administrator creates user accounts for the actors, monitors the processes and performs the analytics. The account/card holder logs in to perform various transaction as allowed him by the system. The class diagram is shown in fig. 4.

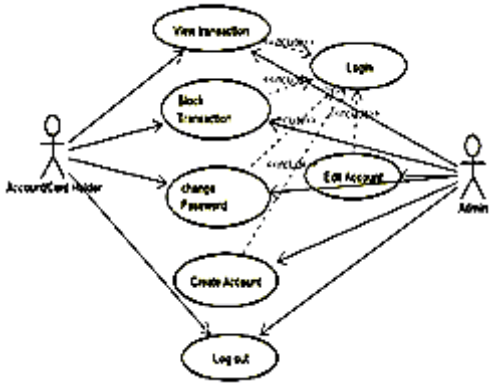

Fig. 3. Use Case Diagram

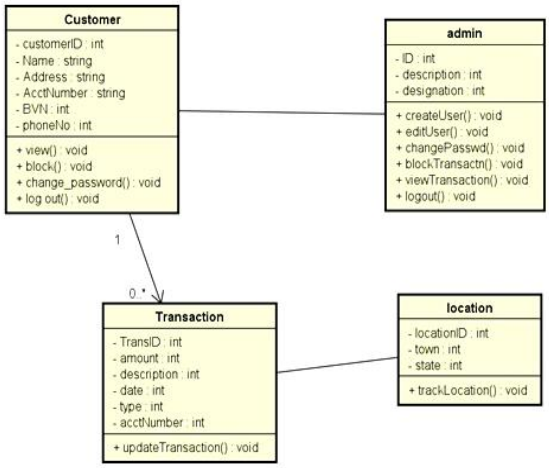

Fig. 4. UML Class Diagrams

IV. RESULTS AND DISCUSSION

The system is a web application and as such consists of so many web pages- home, login, new user registration, admin create account and dashboard pages. The admin and customer dashboards are seen in fig. 5 and fig. 6 respectively.

A. Customers' Dashboard:

In this page, customer has the options of viewing transactions, Block Transaction and Log Out as shown in fig 6. The customer will not affect any change on the transaction log, (crediting and debiting). The essence of

International Journal of Electrical Electronics & Computer Science Engineering
Volume 6, Issue 6 (December, 2019) | E-ISSN : 2348-2273 | P-ISSN : 2454-1222
Available Online at www.ijeecse.com

the program is to give the customer the right to block the account in case of fraud to minimize loss and maximize time. On the block operation icon, the customer has two options, to use the one time password option or to use the bank verification number option as shown in fig 6.

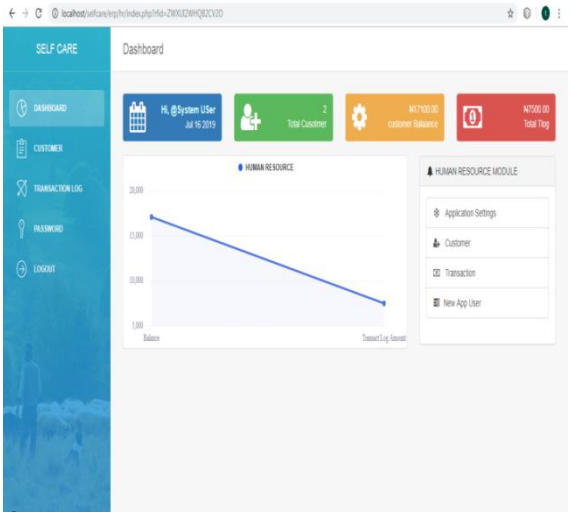

Fig. 5. Admin Dashboard

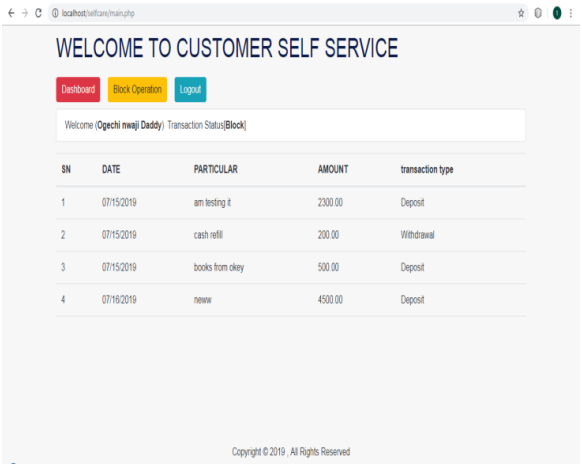

Fig. 6. Customer Dashboard. Customers can view their transaction details while on this page.

B. Admin Dashboard:

The Admin dashboard is where user profile can be edited. It is also where navigation on customers' transactions can be done. We have icons like application setting, where modification can be done on the application. We also have views of total number of customers on the application, customers balance and total transaction log.as shown in fig 5.

C. Comparative Analysis between Existing and Proposed System:

When fraud occurs on credit cards, the negative impact is huge as the financial loss experienced cuts across all the parties involved while the existing system had a thorough work for misclassification, providing a proactive measure/ approach in detecting fraudulent activities regarding the credit card using machine learning known as the cortical learning algorithm to build the credit card fraud detection model. The algorithm worked on the credit card data obtained from the UCI Repository, it converted the highly populated data to a sparse representation, and then used its learning columns to learn spatial and temporal patterns. The object oriented analysis and design methodology was used in the design of the system which was implemented with JAVA programming language. The simulation was carried out with Matlab. Hence, cases of misclassification were reduced to the barest minimum and efficiency of fraud detection was increased.

Table 1. Comparative Analysis of the Existing and Proposed System

SN	Existing System		Proposed System	
1.	Time Complexity (TC)	15	21	Time Complexity (TC)
2.	Life-Cycle Assessment (LCA)	7	15	Life-Cycle Assessment (LCA)
3.	Benchmarking (B)	12	7	Benchmarking (B)
4.	Multi-Criteria Decision Making (MCDM)	15	22	Multi-Criteria Decision Making (MCDM)
5.	Risk Assessment (RA)	10	8	Risk Assessment (RA)
6.	Cost Benefit Analysis (CBA)	8	10	Cost Benefit Analysis (CBA)
7.	Speed	5	12	Speed

The proposed system developed an enhanced credit card transaction for outlier fraud detection system using an artificial neural network algorithm called cortical learning algorithm and customer self-strip detection (OTP, Account Number and BVN) for detecting fraud from the user (the customers) perspective. In the admin column, it converts the highly populated data to a sparse polar representation. Support Vector Machine was used to train active data on the customers' column which is our area of concentration. Object Oriented Analysis and Design Methodology (OOADM) and PHP programming language are used in implementing .MySQL and Simplified unified database are used for NUBAN for every report made from the customer.

Hence dealing with real word situation and having an individual involvement.

V. CONCLUSION

As card business transactions increase, so too do frauds. Clearly, global networking presents as many new opportunities for criminals as it does for businesses. While offering numerous advantages and opening up new channels for transaction business, the internet has also brought in increased probability of fraud in credit card transactions. The good news is that technology for preventing credit card frauds is also improving many folds with passage of time. Reducing cost of computing by helping in introducing complex systems, which can analyze a fraudulent transaction in a matter of fraction of a second.; it is equally important to identify the right segment of transactions, which should be subject to review,

A. Recommendations:

Further work can be done using unstructured Supplementary Service Data (USSD) on a mobile application monitoring transaction to detect and stop credit card outlier (fraud), as every transaction does not have the same amount of risk associated with it. This study provides a low cost approach that can assist acquiring and issuing banks in combating frauds more efficiently it works on real time not stimulated environment. Financial Institution can use this application for upgrade which makes it better involvement of the individual card holder.

B. Contribution to Knowledge:

An Enhanced credit card transaction for outlier fraud detection system using artificial neural network has been developed. This will solve fraud detection and blockage from the customer/individual (User) side. A customer can take action when fraudulent transaction is being perceived or noticed without feeling helpless due to network issues in contacting financial institutions' customer care services department.

VI. REFERENCES

[1] V. Kumar, "Parallel and Distributed Computing for Cybersecurity" Distributed Systems Online, IEEE 6, 10, 2011.

[2] C. Spence, L. Parra, and P. Sajda, "Detection, Synthesis and Compression in Mammographic Image Analysis with a Hierarchical Image Probability Model" In Proceedings of the IEEE Workshop on Mathematical Methods in Biomedical Image Analysis. IEEE Computer Society, Washington, DC, USA, 3, 2011.

[3] E. Aleskerov, B. Freisleben, B. Rao, "Cardwatch: A Neural Network Based Database Mining System for Credit Card Fraud Detection" In Proceedings of IEEE Computational Intelligence for Financial Engineering, 220-226, 2007.

[4] R. Fujimaki, T. Yairi, K. Machida, "An Approach to Spacecraft Outlier Detection Problem Using Kernel Feature Space" In Proceeding of 11th ACM SIGKDD International Conference on Knowledge Discovery in Data Mining. ACM Press, New York, NY, USA, 401-410, 2005.

[5] J. Han, G. Kamber, T. Micheline, "Data Mining: Concepts and Techniques" Morgan Kaufmann. 5. ISBN 978-1-55860-489-6, 2000.

[6] E. M. Knorr, R. T. Ng, "A Unified Approach for Mining Outliers", In Proceedings Conference of the Centre for Advanced Studies on Collaborative Research, IBM Press, 11, 2008.

[7] K. Yamanishi, J. Takeuchi, G. Williams, P. Milne, "Online Unsupervised Outlier Detection Using Nite Mixtures with Discounting Learning Algorithms", Data Mining and Knowledge Discovery 8, 275-300, 2010.

[8] E. Kemmerer, D. Vigna, "A Unified Approach for Mining Outliers", In Proceedings of Conference of the Centre for Advanced Studies on Collaborative Research, IBM Press, 11, 2011.

[9] S. Ghosh, D. Reilly, "Credit Card Fraud Detection with a Neural Network", In Proceedings of the 27th Annual Hawaii International Conference on System Science, Vol. 3. Los Alamitos, CA, 1994.

[10] D. S. Guru, H. S. Nagendraswamy, "Clustering of Interval-Valued Symbolic Patterns Based on Mutual Similarity Value and the Concept of Mutual Nearest Neighbour", In ACCV (2) 234-243, 2006.

[11] D. Ronald M., Daubert, J. Ravkin, H. Lischka, "Keys Making RSA Secured", Review of Policy Research, 29, 1: 5-20, 2010.

[12] M. Davide M. "Graphical Models for Text Mining: Knowledge Extraction and Performance Estimation", Ph.D. Thesis., 2013.

[13] A. K. Jain, Arun Ross, "Introduction to Biometrics", In Jain, AK; Flynn; Ross, A. Handbook of Biometrics. Springer.1–22. ISBN 978-0-387-71040-2, 2008.

[14] M. D. Sahidullah. (2015), "Enhancement of Speaker Recognition Performance Using Block Level, Relative and Temporal Information of Subband Energies", PhD Thesis (Indian Institute of Technology Kharagpur).

[15] E. Mordini, A. Rebera, "No Identification Without Representation: Constraints on the Use of Biometric Identification Systems", Review of Policy Research, 29, 1: 5-20 , 2011.

[16] C. Hordeski, "A Relational Model of Data for Large Shared Data Banks" Communications of the ACM 13,6 :377–87, 1986.

[17] S. Maes, U. Nehmzow, J. Shapiro, J, "A Model of Habituation Applied to Mobilerobots: In Proceedings of Towards Intelligent Mobile Robots, Department of Computer Science, 2002.

[18] A. Neda, L. Akbari, "Choosing an Appropriate Model for Novelty Detection, "In Proceedings of the 5th IEEE International Conference on Artificial Neural Networks", 227-232, 2014.

[19] M. R. Chowdhury, A.S. Ferdous, N. Parvez, S.M. Kamruzzaman, "Text Classification using the Concept of Association Rule of Data Mining", Proc. International Conference on Information Technology, Kathmandu, Nepa, 2010.

[20] Chandrahas Mishra, D. L. Gupta, Raghuraj Singh, "Credit Card Fraud Identification Using Artificial Neural Networks", International Journal of Computer Systems, pp: 151-159, Volume 4, Issue 7, July 2017.

[21] K. C. Philip, J. S. Salvator, "Towards Scalable Learning with Non-Unified Class and Cost Distributions: A Case Study in Credit Card Fraud Detection", IJCS, 10(2), 1998.

[22] Y. Sahin, E. Duman, "Detecting Credit Card Fraud by Decision Trees and Support Vector Machines", International Multiconference of Engineers and computer scientists, 2011.

[23] L.U. Oghenekaro, C. Ugwu, "A Novel Machine Learning Approach to Credit Card Fraud Detection", IJERT 5(6), 52-69, 2016.