An Enhanced Fraud Detection Model using Neural Networks for Telecommunications and Smart Cards in Nigeria

Onuodu, Friday Eleonu & Nnaa, Sunday Barikui

University of Port-Harcourt

ABSTRACT

Fraud, especially smartcard and telecommunication-based fraud always leave a grievous loss to its victims. The banking sector and the telecom companies has battled with this plague for years, fighting it with both technological and other security measures to eliminate its occurrence, but there are still open- problem despite all the efforts. Most of the systems developed are usually reactive instead of proactive, i.e. they detect the fraud after they have already occurred instead of preventing it, and others detect the fraud but do not have the mechanism to prevent it from occurring. Hence, the need for the development of an enhanced model that can detect Smartcard and telecom frauds in real-time and block the transaction while informing the relevant stakeholders (the account owner and the bank). In this work, we used the neural network to train a system using historical dataset of credit card fraudulent transactions and telecom fraud. This system could eliminate the inefficiencies of the existing systems and produced more efficient fraud detection and prevention using the Rule-Based approach to classify suspicious transactions and flag them if they contradict the rules. The result shows that fraud detection can now be made using well prepared datasets. Our model scored a performance accuracy mark of 94% as opposed to the existing system which had 65%.

Keywords: telecommunication, fraud, smart card, detection, neural network (ann).

Classification: F.1.1

Language: English

London
Journals Press

LJP Copyright ID: 975841
Print ISSN: 2514-863X
Online ISSN: 2514-8648

London Journal of Research in Computer Science and Technology

Volume 20 | Issue 2 | Compilation 1.0

An Enhanced Fraud Detection Model using Neural Networks for Telecommunications and Smart Cards in Nigeria

Onuodu, Friday Eleonu[α] & Nnaa, Sunday Barikui[σ]

ABSTRACT

Fraud, especially smartcard and telecommunication-based fraud always leave a grievous loss to its victims. The banking sector and the telecom companies has battled with this plague for years, fighting it with both technological and other security measures to eliminate its occurrence, but there are still open-problem despite all the efforts. Most of the systems developed are usually reactive instead of proactive, i.e. they detect the fraud after they have already occurred instead of preventing it, and others detect the fraud but do not have the mechanism to prevent it from occurring. Hence, the need for the development of an enhanced model that can detect Smartcard and telecom frauds in real-time and block the transaction while informing the relevant stakeholders (the account owner and the bank). In this work, we used the neural network to train a system using historical dataset of credit card fraudulent transactions and telecom fraud. This system could eliminate the inefficiencies of the existing systems and produced more efficient fraud detection and prevention using the Rule-Based approach to classify suspicious transactions and flag them if they contradict the rules. The result shows that fraud detection can now be made using well prepared datasets. Our model scored a performance accuracy mark of 94% as opposed to the existing system which had 65%. This work could be beneficial to telecom industries, to banks, to users of smartcards and POS and to every other person who carries out cashless transactions via the smartcards.

Indexterms: telecommunication, fraud, smart card, detection, neural network (ann).

Author α: Department of Computer Science, University of Port-Harcourt, Rivers State Nigeria.
σ: Department of Computer Science, Ignatius Ajuru University of Education, Rivers State, Nigeria.

I. BACKGROUND

Fraud is a major problem that the world is facing today. It can actually be classified as a disaster due to the devastating effects it has on its victims [1].Fraud has crept into all the sectors of the countries of the world and into almost all human activities and transactions with each other. From the activities of con artists, to forgery of documents, manipulation of records etc. over the years, several technologies for fraud detection have been developed in order to detect and prevent fraudulent activities in various sectors of the economy especially in the financial sector. In fact, once a technology emerges, the next step will be to build a strong fraud detection and prevention system that will work with the system to cushion and prevent fraudsters from accessing such technologies and carrying out fraudulent activities on them. Sometimes, most of the emerging technologies also have inbuilt fraud detecting mechanisms with them. However, some frauds are still hard to detect using the current technical security measures, especially in the telecommunication and smartcard based industries [2].

Telecommunication is a brilliant technology that has impacted the lives of almost all the citizens of the world as it aids communication across the globe, “In fact it is turning the world into a global village” [3]. This technology has experienced an increased acceptance across the world and this has led to a tremendous growth in the industry.

Innovations in the industry are also very frequent with new emerging technologies almost every day. The telecommunication community attends to the needs of two kinds of users, those who are provided with connections at an affordable rate also called the domestic users, and the second set are those who are provided with connections at a higher rate because of the higher scale of usage and subscription by these users, they are called the commercial users. However, over the years it has been noticed that the domestic users purchase subscriptions meant for the commercial users and vice-versa fraudulently. This is where the problem of fraud in the telecommunication industry and it has caused a great loss instead of profit to the sector. Another scenario of fraud is the telecom industry is when the users intentionally transmit voice data across a telecom network with the aim of avoiding or reducing the normal call charges. Abuse of voice and data networks are also fraudulent activities carried out on the telecom network.

In the case of credit card/smartcard fraud, it is normally and mostly noticed in the financial industries which inculcate technologies such as the electronic banking. The financial industry has suffered severe loss in the hand of the fraudsters over the years. Detecting the fraud has been a difficult task because, the pattern used in executing the fraud are not continuous, as they change from time to time. Once and again, a measure for detecting the financial fraud using the smartcards have been developed, but instead of curbing the attack, the fraudsters will always develop another pattern for carrying out fraudulent activities. The smartcard technology is another widely accepted technology due to its relevance in the implementation of a “cashless society” policy, however, these attacks on the users is posing a big threat to its continuous advancement as the customers are beginning to doubt the safety of their transactions using smartcards. The effect of fraud on smartcards affects both the users and the financial institutions, losses ranging from lawsuits by the customers who have been defrauded are becoming a normal occurrence in this industry. Research has it that the increase in technological advancement of the world is directly proportional to the increase in fraud in such sectors.

The use of artificial neural network (ANN) adds a true artificial intelligence to the security defences of the system, rather than the security measures that have been previously implemented. The ANN can be extremely helpful in modelling a complex transactional pattern. Therefore, it is suitable for a smartcard and telecommunication fraud detection system.

1.1 Aim and Objectives

The aim of this work is to develop an enhanced fraud detection model using neural networks for the telecommunication and smartcard in Nigeria. The specific objectives are to:

i. Design a secure smartcard and telecom transaction platform for new and existing users of the smartcard and telecom technologies.
ii. Develop fraud detection system that will diagnose and block suspected fraudulent activities via the smartcard and telecom platform
iii. Implement with Hypertext Pre-processor (PHP), JavaScript (JS), Hypertext Markup Language and MySQL as backend.
iv. Compare result with the existing system performance.

1.2 Credit Card Fraud

Fraud can be classified as any activity with the intent of deception to obtain financial gain by any manner without the knowledge of the cardholder and the issuer bank. Credit Card fraud can be done in numerous ways.

Credit card fraud has been causing many financial losses for the customer and the organization. In recent years this subject has been a growing line of research, techniques such as machine learning are used to detect and block fraudulent transactions.

According to the Federal Trade Commission of the United States, figures on fraud and credit card identity have been increasing in recent years, with 13 million of claims from 2012 to 2016 of its online database of consumer complaints. Statistics on Credit Card Fraud registered 1.3 million complaints in 2016, corresponding to 42 % of total complaints [4]

Recognizing misrepresentation or fraud is a difficult issue since fraudsters cause their conduct to seem real. Another trouble is that the quantity of real records is far more noteworthy than the quantity of false cases. Such unequal sets require extra safety measures from the information expert. The way to exact extortion location lies in the improvement of dynamic frameworks that can adjust to new fraud pattern or designs [5]

Fraud detection involves discovering a fraud activity in the midst of thousands of authentic ones, which could be very difficult and challenging. "With continued advancement in fraudulent strategies it is important to develop effective models to combat these frauds in their initial stage only, before they can take to completion" [6] The big challenge in developing such a model is that the number of fraudulent transactions among the total number of transaction is a very small number and hence the work of finding a fraudulent transaction in an effective and efficient way is quite perplexing.

Some common types of credit card fraud include:

- *Application Frauds:* This occurs when the fraudster gains control of the application system by accessing sensitive user details like password and username and open a fake account. It generally happens in relation to the identity theft. When the fraudster applies for credit or a new credit card altogether in the name of the cardholder. The fraudster steals the supporting documents in order to support or substantiate their fraudulent application.
- *Electronic or Manual Credit Card Imprints:* When the fraudster skims information that is placed on the magnetic strip of the card. This information is very confidential and by accessing it the fraudster may use it for fraudulent transactions in future
- *CNP (Card not Present):* When the fraudster knows the expiry date and account number of the card, the card can be used without its actual physical possession.
- *Counterfeit Card Fraud:* It is generally attempted through the process of skimming. A fake magnetic swipe card is made and it holds all the details of the original card. The fake card is fully functional and can be used to commit transactions in future.
- *Lost and Stolen Card Fraud:* In cases when the original card holder misplaces their card, it can get to the hands of fraudsters and they can then use it to make payments. It is hard to do this through machine as a pin number is required however; online transactions are easy enough for the fraudster.

1.3 Detecting Credit Card Fraud using Neural Networks

An artificial neural network (ANN) is a lot of interconnected hubs intended to copy the working of the human mind (Ghosh and Reilly, 1994). Every node has a weighted association with a few different nodes in contiguous layers. Singular nodes or hubs take the information got from associated nodes and utilize the loads together with a straightforward capacity to figure yield esteems. Neural systems or network architecture come in numerous shapes and designs. The Neural system design, including the quantity of shrouded layers, the quantity of nodes inside a particular concealed layer and their availability, most be indicated by client dependent on the intricacy of the issue.

The standard of neural network is roused by the elements of the brain particularly pattern acknowledgment or recognition and acquainted memory. The neural network perceives comparable patterns, predicts future qualities, values, or occasions dependent on the affiliated memory of the pattern it was learned. It is broadly applied in order and grouping. The benefit of neural network over different procedures is that these models can gain from an earlier time and hence, improve results over the long haul. They can likewise extricate rules and anticipate future movement dependent on the present circumstance. By utilizing neural systems, viably, banks can distinguish deceitful utilization of card, quicker and even more proficiently. Among the revealed credit card fraud considers most have concentrated on utilizing neural networks. In progressively reasonable terms, neural networks are non-direct factual data modelling apparatuses or tools. They can be used to model complex connections among information sources and yields or to discover designs in the information. [7].

There are two stages in neural network training and acknowledgment [7]. There are two types of neural network (NN) training methods regulated and unregulated methods. In regulated training method, samples of both fake and non-deceitful records used to create models. The regulated training method just looks for that transaction, which is generally divergent from the standard. On the other hand, the unregulated training methods do not need to bother with the past information on fraudulent and non-fraudulent transactions in the database. Neural networks (NNs) can deliver the best outcome for just enormous transaction dataset. They need long training dataset.

One of the merits of utilizing unsupervised neural networks over similar techniques is that these techniques can learn from data stream. The more information went to a SOM model, the more adjustment and enhancement for result is obtained. All the more explicitly, the SOM adjusts its model over the long haul. Accordingly, it can be utilized and updated online in banks or other money related enterprises. Subsequently, the fraudulent utilization of a card can be recognized quick and successfully.

In any case, neural systems have a few disadvantages and challenges, which are predominantly identified with determining appropriate engineering in one hand and over the top preparing required for coming to best execution in other hand.

1.4 Telecommunication Fraud

The telecommunication industry has extended significantly over the most recent couple of years with the advancement of reasonable cell phone innovation [8]. With the expanding number of cell phone supporters worldwide, cell phone fraud is likewise set to rise. It is an overall issue with significant yearly income misfortunes of numerous organizations. Media transmission fraudulent which is the centre is engaging especially to fraudsters as calling from the portable terminal is not bound to a physical area and it is anything but difficult to get a membership. This gives a way to illicit high benefit business for fraudsters requiring negligible speculation and moderately generally safe of being captured. Telecommunication fraud is defined as the unapproved use, altering or control of a cell phone or administration.

The procedure starts with social occasion verifiable information on fraudulent and non-fraudulent calls. This data is pre-processed to make it reasonable for neural network learning. Next, the neural network is prepared utilizing the pre-processed information to construct a model, which consolidates various examples of false conduct. The model is applied to approaching business where it adaptively learns new examples of misrepresentation improving its model as the kinds of extortion advances. Fraud discovery mechanism might be home blend, exclusive or a blend of both which is most likely the most advantageous methodology [9].

The self-learning framework or system furnishes the general system with the ability to take in new standards about fraudulent from the submission of fraudulent and non-fraudulent space explicit data and naturally distinguish sporadic perceptions in the data in this manner giving an input system to advancing and refreshing the vault of rules. Self-learning system coordinates reasonable calculations for measurable information examination and information mining undertakings that empower it to refresh, improve and expand existing misrepresentation discovery administers by dissecting submitted information. The extortion recognition territory is a functioning region of improvement for neural systems in broadcast communications. A large number of the best frameworks are crossover systems, which exploits the overall qualities of a few AI advances. Given the adjustments included, it is an application, which should come into routine use in the years ahead.

II. RELATED WORK

Jain [6] proposed a comparative analysis of various credit card fraud detection techniques. They discussed various credit card related frauds and provided a concrete review of the various techniques that are currently in place for detecting the frauds. Some of the techniques discussed include the Support Vector Machine (SVM), Artificial Neural Network (ANN), Bayesian Network etc. they analyzed the existing techniques based on quantitative measurements such as rate of detection and the rate of false alarm witnessed with the existing techniques. From their analysis, they arrived at a conclusion that the techniques were not able to detect all types of credit card fraud and when they did they detected the fraud after it has already been perpetrated and not in real time. Also these techniques were not properly trained in order to block fraudulent transactions. Finally, the techniques also lacked cross platform adaptability quality.

Kabari [3] proposed the telecommunications subscription fraud detection using the artificial neural network. They presented the design and the implementation of the fraud detection system in the work. They used Neuro-solutions for Excel to implement the ANN. Their system was subjected to performance testing and was discovered to be user friendly and recorded an 85.7% success and accuracy rate.

Johnson [10] proposed a Medicare fraud detection system. The system was implemented to detect the fraudulent activities carried out within the medical sector, in terms of falsification of health record and insurance records. They evaluated the performance of six deep-learning methods for addressing class imbalance using the CMS medical care data and LEIE fraud labels. They also considered a range of class distribution and studied the relationship between minority class size and the optimal division threshold.

Singh [11] proposed the electronic credit card detection system by collaboration of machine learning models. They focused on fraud activities that cannot be detected manually by carrying out research. They used a dataset of electronic payment card holders. Then they applied the machine learning techniques on the unstructured and process free data.

Malek [2] proposed a fraud detection and prevention in smart card based environments using Artificial intelligence. They considered the possibility of implementing neural network fraud engine on a smart card platform. The system was smart enough to suspend and block any suspicious or unusual fraudulent activity. The usage characteristics of the users were used as parameter for detecting fraud that is connected to the users. Java card 2.1 compliment was used for implementing the fraud engine. The system was tested on a simulator machine implemented on the PC. The engine had an execution time of 4.24 ms which was achieved bt recording 500 runs at 2.12 seconds. However, the execution time was too slow for effective fraud detection. This implies that a smart fraudster would successfully perpetrate his fraud and go uncaught before the system can detect it.

Oumar and Augustin [1] proposed credit card detection using ANN. In their work, data consisting of fraudulent and non-fraudulent activities were used as parameters to detect future fraud. The parameters were used to create a model that classifies the transaction with a high accuracy based on a machine learning technique.

ANN with Logistic Regression were used as a means of measurement and in order to achieve high accuracy, they refined the model using Back propagation which had proved to record high accuracy in time passed in order to help the model differentiate between fraudulent and non-fraudulent activities. However, their models are too ambiguous and not time and cost efficient.

Amanze and Onukwgha [12] proposed a review of the credit card fraud detection system for Nigerian banks using Adaptive mining and intelligent agents. They were able to design and implement a credit card fraud detection system for the banking industry in Nigeria. Their model consisted of a hybrid model which combines evidence from current and previous transaction behaviours of the customer in order to detect the suspicion level of each incoming transaction. Their research also gave a statistics of the fraud rate in Nigeria via credit card transaction. However, their fraud detection accuracy was low and called adequate improvement by the use of better models and algorithms for the system's implementation.

Amanze [13] proposed accredit card fraud detection system using intelligent agents and enhanced security measures. The aim of the system was to detect the fraud while it is going on by sending a token to the customer and for more security checks, the system would also ask the user secret questions which only the users can provide answers to. If the answers provided are correct, the transaction will be flagged as successful. But if the answers are wrong, the transaction will be tagged as fraudulent and an SMS will be sent to the customer and the bank to notify them of the fraudulent activity. However, this system does not automatically block confirmed fraudulent transactions but waits for the customer and the bank to take actions on the fraud detected. This system basically just provides information about proposed fraud and does nothing else about it.

Daliri [14] proposed a study that uses harmony search algorithm in neural networks to improve fraud detection in the banking system. In the proposed method, hidden patterns between the fraudulent and non-fraudulent customer's information were searched. This system detects the fraudulent activity and immediately blocks it before it takes place. The approach of this system was considered to be the best because of its proactive nature which is a booster for every fraud detection system. However, the system design of this system is ambiguous and time consuming, it is also not cost efficient for small scale developers.

Delamaire [15] proposed a study to discuss credit card fraud detection techniques. In their study, they pointed out different types of credit card fraud by reviewing several articles on credit card fraud. Then, they identified the available techniques at that time for detecting credit card fraud. Some of the fraud types identified were bankruptcy fraud, counterfeit fraud and behavioural fraud. Some of the prescribed techniques were the genetic algorithm, clustering techniques, neural networks, pair-wise matching and the decision tree. However, they could not build a suspicion scorecard that can predict fraudulent behaviours while taking into account the field of behaviour that can relate to the various types of credit card fraud.

Zanin [16] proposed credit card fraud detection through parenclitic network analysis. They presented a "a first hybrid data mining complex network classification algorithm", which had the capability to probe and discover fraudulent instances in a real card transaction dataset. Their decision to use that particular model was as a result of a network reconstruction algorithm that allowed representation of the derivation of one instance from a reference group to be created. They demonstrated how addition of features derived from a network data representation improved the score obtained by a standard neural network-based classification algorithm and additionally how this combined approach can out performs a commercial fraud detection system in certain operation niches. They also tested the feasibility of using complex networks to improve data mining model. However, their model could not detect credit card fraud such as bankruptcy fraud and other difficult credit card fraud that seem difficult to detect.

Zhang [17] proposed a model based on convolutional neural network for online transaction fraud detection. They presented a model for detecting fraud in the field of online transaction using the convolutionary neural network which constructs an input feature sequencing layer that implements the reorganization of raw features from different feature combination entering the convolution kernel to form different convolutional patterns. The model could collect low and non-derivative online data as input. The whole network consisted of a feature sequencing layer, four convolutional layers and pooling layers, and a fully connected layer. The system was tested using online transaction data from the commercial bank. Though their system produced a great accuracy rate in detecting fraud up to 94% according to their evaluation, however, they did not pay more attention to the discovery of sequence characteristics of transactions.

Sadgali [18] proposed fraud detection in credit card transaction using neural networks. They examined three advanced data mining techniques namely neural networks (NN), multiplayer perceptron layer (MPL) and convolutionary neural networks (CNN). They used a unique generic credit card dataset to evaluate the performance of their model. In the evaluation they compared and analysed each of the technique. After the analysis, they postulated that the MLP was best for detecting credit card fraud when applied to the generic dataset used. However they could not present a complete architecture of an adaptive model for credit card fraud detection using the result of their analysis.

Abakarim [19] proposed an efficient real time model for credit card fraud detection based on deep learning. Their model was based on an auto-coder that permits classification in real time credit card transaction as either genuine or fraudulent. Four different models classification models were used as a comparison to test the efficiency of their model. In terms of accuracy, recall and precision, benchmark showed better results for their model than those existing at that time since it recorded the F1 score.

III. MATERIALS AND METHODS

3.1 Methodology

We adopted System Development Lifecycle Methodology (SDLC) in this approach.

3.2 Analysis of the Existing System

Their dissertation focused on credit card application which was used to detect the fraudulent credit card activities on credit transaction. In this peculiar type, the pattern of current fraudulent usage of the credit card was analyzed with the previous transactions, by using the intelligent agent in data mining algorithm. Fig. 3.1 shows the architecture of the existing system model. The system has three data mining engines: customer/bank database, credit card transaction database and fraud detection database. The customer/bank database had the following: opening of account operation, withdrawal and deposit transaction and credit card transaction. Fraud techniques database gave details of attack attempts on customer's credit card. The credit card database contained all the previous credit card transactions carried out by the customer. The existing Credit Card Fraud Intelligent Agent Model (CCFIAM) was to detect the credit card fraud by analysing the spending patterns on every card and figure out any inconsistency with respect to the usual spending patterns. Intelligent agent was made use of these inputs (from user transaction input and past recorded credit fraud detection input) and watched ongoing transaction to check whether is fraudulent or not, beginning from the most recent attack methods of fraudsters and concentrating the most recent spending pattern of the transaction.

In the existing system, when a credit card transaction is initiated, the system verifies the user's pin code and username by validating it on the bank database. If the pin fails to validate after three consecutive attempts, the transaction was denied and fraud alert sent to the fraud database. But if the pin verification was successful, the system will capture the credit card transaction details and verify the credit card information before passing the information to data monitoring agent.

The monitoring agent used the last ten credit card transaction to build a transaction pattern for the customer and forward the pattern to the collating agent. The Monitoring agent also used data mining technique to retrieve previous credit card fraud patterns from the credit card database and also retrieve the customer details from the bank database. At monitoring agent, each of the agents focused on a particular type of credit card fraud, the agents ran in parallel and reported any suspicious attack to collating agent. However, the collating agent was responsible for communication with the diagnosing agent, which includes sending the task to be performed as input and providing the required data. The diagnosing agent matched the existing pattern of credit card transaction with the new transaction to check if there are variations in the pattern. If the transaction pattern does not match, the system will request for a secret question and answer from the user for more authentication. If the user fails the question, a fraud alert is send to the reporting agent. The reporting agent will then forward the extracted credit card transaction status to the database of the bank and the customer's phone and the transaction is denied. But where the credit card profile matched with the existing customer profile, the transaction is allowed to go through and the customer's account updated. At this, the transaction will be recorded on the credit card database and the fund transferred will be deducted from the customer's account balance.

3.2.1 Explanation of the Existing System Components

i. *Intelligent Agent:* These agents were responsible for ensuring that the transaction carried out via the credit card are by a valid user by ensuring that the details of the transaction are valid, detecting any suspicious activity and reporting them to the original owner of the account and the bank also.

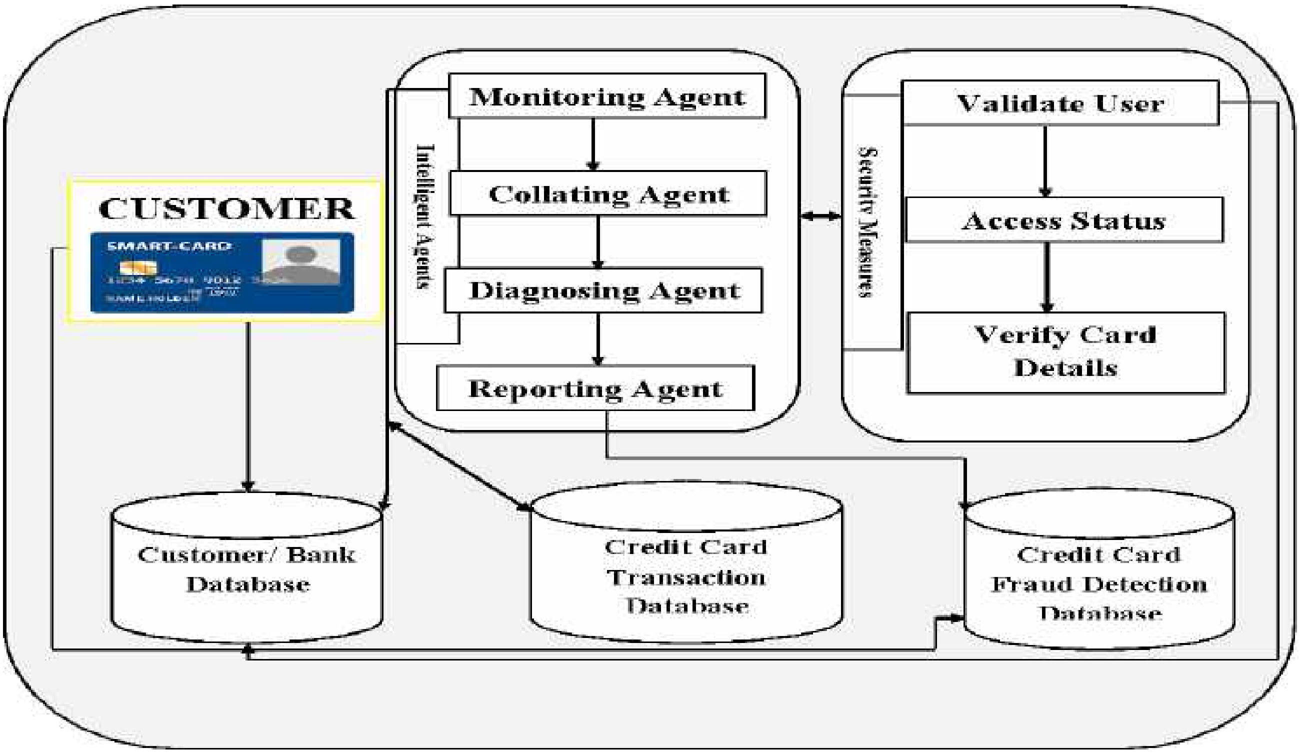


Fig.3.1: Cradit Card Fraud Detection System Using Intelligent Agents And Enhanced Security Features (Existing System.Source:Amanze[13])

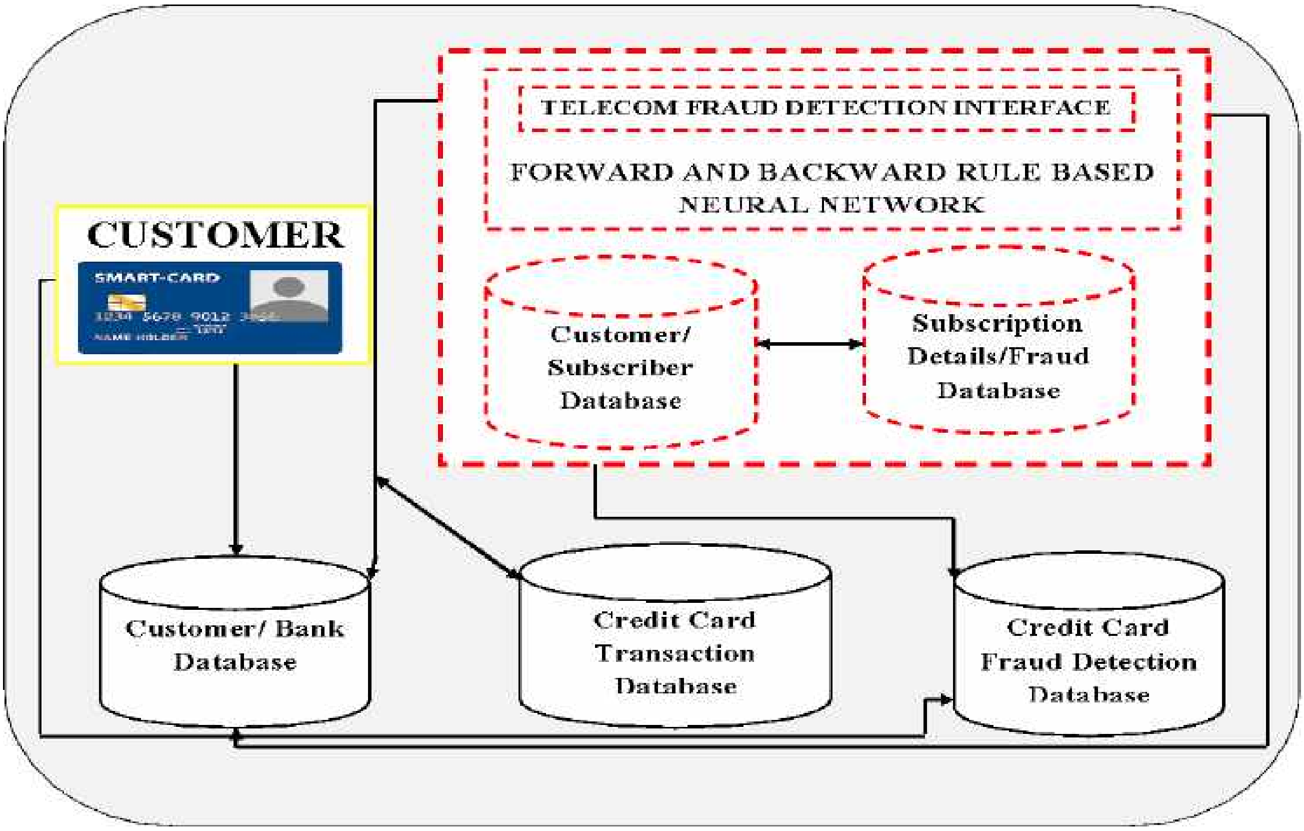

TELECOM FRAUD DETECTION INTERFACE
FORWARD AND BACKWARD RULE BASED NEURAL NETWORK
CUSTOMER
SMART-CARD
1234 5678 9012 3456
NAME HOLDER
Customer/ Subscriber Database
Subscription Details/Fraud Database
Customer/ Bank Database
Credit Card Transaction Database
Credit Card Fraud Detection Database

*Fig.3.2:*An Enhancedfraud Detection Model Using Natural Networks For Telecom And Smartcards(Proposed System)

ii. *Security Measures:* These were measures put in place to aid the user interact with information on his/her account and to view the activities on his account. It also helps the system to confirm that the information provided by the user corresponds to the one previously stored.

iii. *Customer:* This phase introduces the user of the smartcard at the time. The user uses the smartcard to initiate a transaction which will either be flagged as successful or otherwise depending on the security check results of the system.

iv. *Customer Bank Database :* The customer/bank database has the following: opening of account operation, withdrawal and deposit transaction and credit card transaction. Details of the customer's personal information and secret pin are some of the data that are stored in this database.

v. *Credit Card Transaction Database:* The credit card database will contain all the previous credit card transactions carried out by the customer. Once a new transaction was carried out, whether successful or not, it was automatically be stored in this database.

vi. *Fraud Detection Database:* Fraud techniques database will gave details of attack attempts on customer's credit card. Details such as the time, date and at which service point the fraudulent activity was perpetrated will be stored in this database.

3.2.2 Advantages of the Existing System

i. The adaptive data mining and intelligent agent's model introduced a more secured communication channels for credit card transactions thereby preventing loss of money by the customers to credit card fraudsters.

ii. The existing system provided a kind of confidence in the customers that they are sending their personal information to legitimate banks' servers and not impostors. This helped to boost the electronic transactions thereby reducing the queue in the banking halls.

iii. The fraud detection system ensured that all critical data (credit card numbers, for example) were encrypted and that only authorized users have access to data in its entirety.

iv. The existing system was featured with alert system to enable e-commerce owners receive alert of fraudulent activities and automatically disable customer's (victims) account involved.

3.2.3 Disadvantages of the Existing System

i. The existing system's security measure for checking and detecting fraudulent activity is not effective enough to detect the recent forms of credit card fraud.

ii. The system does not provide any measure to detect telecommunication fraud in their system design.

iii. The execution time of the existing system is not fast enough to detect fraud in real time and the system does not include measures to block the credit card fraud account after two unsuccessful tries.

3.3 Analysis of the Proposed System

The proposed system is an enhanced fraud detection model using neural networks for telecommunication and smart cards. It is an improvement of the work carried out by Amanze [9]. the proposed system is a reliable smartcard and telecommunication fraud detector, due to the use of neural networks to train the system based on historical data from customer smartcard transaction, historical subscription details, and credit card fraud technique database. The proposed system follows the same principle of the existing system, but uses a better model based on neural network to detect fraudulent activities. The customer/bank database has the following: opening of account operation, withdrawal and deposit transaction and smartcard transaction. Fraud techniques database gave details of attack attempts on customer's smartcard. The smartcard database will contain all the previous credit card transactions carried out by the customer.

For the telecommunication fraud detector, the historical data is collected and normalized to reduce redundancy in the data and then used to train the system based on set of specified rules which will be specifies by the system. The rules are stored in database of rules and the system will always refer to these rules to classify a transaction as fraudulent or not. If a user initiates a subscription request, the user's details are checked against the details in the historical user details dataset, if the details match, then the user will be further verified to check if it's a domestic or commercial user. The domestic are usually provided with connections at an affordable rate, and the commercial are provided with connections at a higher rate because of the higher scale of usage and subscription by these users. This also implies that the commercial users will request for higher data subscription plans that the domestic users. Therefore, once the subscription request is launched by the subscriber, the system will use the information provided by the subscriber to verify if it's a domestic or commercial user. If the user is a domestic user and has requested for the connections and subscription of the commercial user, the system will flag the request as unsuccessful and will block the user's access to that particular service provider upon more than three retries.

On the other hand, for the smartcard user, the customer is assumed to have previously registered and has his/her details saved before being issued the smartcard by his/her bank. Also his transaction activities on that card has been monitored and saved. If the user launches a request to use the card either for withdrawal or to purchase an item, the secret pin will be required, if the user provides the correct pin in two trials, the transaction will be flagged successful. However, if the pin entered is incorrect twice, the transaction will first be flagged unsuccessful, and user will be referred to a page where he will be required to provide sensitive personal information that can only be known by the user, if the user successful supplies these answers, he/she will be required to reset his secret pin to the one he can remember and then retry the transaction which will now be successful. Else, the transaction will be tagged as fraudulent and blocked.

In this proposed system, the forward and backward rule based neural network is used to train the system to detect and block fraudulent activities on smartcard and telecom services in realtime before they even occur. The rule based approach works in the hidden layer of the neural network to work on the input available (historical dataset) to train the input in order to achieve accurate classification of transactions and detections if any is suspected to be fraudulent.

3.3.1 Explanation of the Proposed System Components

i. *Telecommunication Fraud Interface:* This provides an interface for the user to request for data subscriptions from his service provider. On the side of the service provider, i.e. the telecom service provider, they use this platform to verify the user and his request.

ii. *Neural Network:* This model helps to verify a users transactions using a set of laid down rules (**"ifs"**), it helps to train the system to classify user transactions as authentic or fake based on laid down rules already specified and used to train the system.

iii. *Customer / Subscriber Database:* This component consists of three vital phases known as the distribution phase which distributes letters, words and lines for the analysis and interpretation in a specific order. The disposition phase involves the disposition of texts within the page taking into account the four margins, (page margins; sides of the page each have a meaning) that must be large enough cared for with a harmonic heading. Furthermore, the proportion phase is the equilibrium of the dimensions of letters between each other. It means there is equilibrium in sense of humor and judgment upon judging.

iv. *Subscription Details / Fraud Database:* This database contains all the previous subscription activities of the user of the SIM. It also contains all the details of the fraudulent activities carried out via the SIM card.

3.3.2 Advantages of the Proposed System

The following advantages of the Proposed System include the:

i. The forward and backward rule based neural network model introduced a more secured transaction using telecommunication and smartcard based services to prevent losses to fraudsters..

ii. The proposed model boots the confidence of smartcard users due to the assurance that any suspected fraudulent activity on their account will be blocked without their participation and that their money will not be accessed without their permission.

iii. The fraud detection system ensures that all critical data (credit card numbers, for example) were protected and that only legitimate users have access to the data.

iv. The proposed system was featured with alert system to enable the users and the service providers (banks and telecom companies e.g. MTN) receive alert of fraudulent activities and then perform certain operation to ensure that the customer's data and resource is protected and safe.

v. The proposed system automatically blocks all suspected fraudulent activities in realtime before they can even occur. Hence, is the most efficient solution to telecom and smartcard based fraud.

3.4 Existing System Algorithm

Step 1:

To Identify The Profile Of Cardholder From Their Purchasing

Step 2:

The Probability Calculation Depends On The Amount Of Time That Has Elapsed Since Entry Into The Current State.

Step 3:

To Construct The Training Sequence

For Training Model

```
1.  /*initialization*/
2.  S = { };
3.  For (a ∈ Accts) Do Cover [a] = 0;
4.  For (r ∈ Rules) Do
5.  Occur[r] = 0; /*number Of
6.  Accounts In Which R Occurs* Acctsgen[r] = {
    }; /*set Of Accounts Generating R */
7.  End For
8.  Check The Previous Spending
9.  Profile
10. For (a ∈ Accts) Do
11. Ra = Set Of Rules Generated
12. From A;
13. For (r ∈ Ra) Do
14. Occur[r] : = Occur[r] + 1;
15. Add A To Acctsgen[r];
16. End For; End For
17. If Transaction Is Outside Spending Profile
    The Send Alert To Monitoring Agent
18. For (a ∈ Accts) Do
19. Ra = Secret Questions;
20. Request For User To Supply Secret Question
    And Answer
21. While (cover [a] <trules) Do
22. R = Correct From Ra
23. Remove R From Ra
24. If (r ∉ S And Occur[r] ≥ Taccts ) Then
25. Add R To S; 24. For (a2 ∈acctsgen[r]) Do
26. Cover [a2] = Cover[a2] + 1; 26. End For; End
    If
27. End While; End For Intelligent Agents
    Report Back To Transaction Agent If Any
    Rule Is Broken Transaction Agent Stores The
    Alert Received Monitoring Agent Supervised
    By Manager Or Rollback The Transaction
    Before Being Committed To Database
```

Detection Phase: Fraud Detection

Step 1:

To Generate The Observation Symbol

Step 2:

To Form New Sequence By Adding In Existing Sequence

Step 3:

To Calculate The Probability Difference And Test The Result With Training Phase

Step 4:

Finally, If Both Are Same It Will Be A Normal Customer Else There Will Be Fraud Signal Will Be Provided.

3.5 Proposed System Algorithm

Step 1:

To Identify The Profile Of Cardholder From Their Purchasing

Step 2:

The Probability Calculation Depends On The Amount Of Time That Has Elapsed Since Entry Into The Current State.

Step 3:

To Construct The Training Sequence For Training Model

1. /*initialization*/
2. S = { };
3. For (a ∈ Accts) Do Cover [a] = 0;
4. Set Rules For Transactions
5. For (r ∈ Rules) Do
6. Occur[r] = 0; /*number Of Accounts In Which R Occurs*/
7. Acctsgen[r] = { }; /*set Of Accounts Generating R */
8. If Transaction Is Outside Spending Profile The Send Alert To Monitoring Agent
9. Request For Secret Pin To Proceed
10. If Secret Pin = Incorrect * 2
11. Flag Transaction As Unsucessful
12. For (a ∈ Accts) Do
13. Ra = Secret Questions;
14. Request For User To Supply Secret Question And Answer
15. While (cover[a] <trules) Do
16. Suggest Secret Pin Reset
17. Else
18. If (ra. Answer ∉ Answer) Then
19. Block Transaction In Realtime Before It Occurs While System Report Back To Transaction Agent If Any Rule Is Broken Transaction Agent Stores The Alert Received Monitoring Agent Supervised By Manager Or Rollback The Transaction Before Being Committed To Database
20. Else If Secret Pin = Correct Do
21. Execute Transaction

Step 4:

Store All Information In Their Respective Databases

Step 5:

Repeat Step 1-5 For New User Until New Transaction = 0.

Step 6:

Quit.

Telecom Fraud Detection Phase:

Step 1:

Login

Step 2:

Request For Connection Via Subscription

Step 3:

Verify Status Of User (domestic/commercial)

Step 4:

If Domestic User Request = Sm (small Connection) Then

Subscription = Successful. Else

Request = Unsuccessful

Step 5:

Flag Transaction As Fraudulent

Step 6:

Block Transaction.

Step 7:

Store Transaction In The Fraud Database

Step 8:

Quit.

IV. RESULTS AND DISCUSSION

4.1 Choice and Justification of Programming Language used

We implemented the Proposed System design with PHP, JavaScript Programming Language, Hypertext Markup Language, Cascading Style Sheet and MySQL Relational Database Management System. Javascript is a dynamic computer programming language. It is lightweight and most commonly used as a part of web pages, whose implementations allow client-side script to interact with the user and make dynamic pages. It is an interpreted programming language with object-oriented capabilities. JavaScript was first known as LiveScript, but Netscape changed its name to JavaScript, possibly because of the excitement being generated by Java. JavaScript made its first appearance in Netscape 2.0 in 1995 with the name LiveScript.

The general-purpose core of the language has been embedded in Netscape, Internet Explorer, and other web browsers. JavaScript is a lightweight, interpreted programming language, designed for creating network-centric applications, complementary to and integrated with Java, complementary to and integrated with HTML, open and cross-platform

PHP is a programming language for building dynamic, interactive Web sites. As a general rule, PHP programs run on a Web server, and serve Web pages to visitors on request. One of the key features of PHP is that you can embed PHP code within HTML Web pages, making it very easy for you to create dynamic content quickly. PHP is a server-side, HTML-embedded scripting language that may be used to create dynamic Web pages. It is available for most operating systems and Web servers, and can access most common databases, including MySQL. PHP may be run as a separate program or compiled as a module for use with a Web server.

MySQL is a fast, easy-to-use RDBMS being used for many small and big businesses. MySQL is developed, marketed and supported by MySQL AB, which is a Swedish company. MySQL is becoming so popular because of many good reasons: MySQL is released under an open-source license. So you have nothing to pay to use it. MySQL is a very powerful program in its own right. It handles a large subset of the functionality of the most expensive and powerful database packages. MySQL uses a standard form of the well-known SQL data language. MySQL works on many operating systems and with many languages including PHP, PERL, C, C++, JAVA, etc. MySQL works very quickly and works well even with large data sets. MySQL is very friendly to PHP, the most appreciated language for web development. MySQL supports large databases, up to 50 million rows or more in a table. MySQL is customizable. The open-source GPL license allows programmers to modify the MySQL software to fit their own specific environments.

4.2 Discussion of Results

Fig 4.1 shows the home page of the fraud detection system. It contains navigation buttons for accessing either of the two fraud detection system. From this page, a user can carry out either a telecom subscription transaction or a smartcard based transaction. Fig 4.2 contains the welcome page for the telecoms services. Users who intend to subscribe their phones and other devices will click on the manage subscription button to navigate to the subscription request page.

The request page contains a form that the user will be required to fill. Some of the labels of the form include the customer type and the amount of the subscription (in Naira). When a user submits this form, the system automatically verifies the information provided with that stored in the database, the first rule is to verify if the user actually exists, the second rule is to verify that the user is requesting for the subscription that is suited for his type of user.

If the user passes the second rule, the output as shown in Fig 4.3 is gotten and the transaction is the request is granted and tagged as a successful request.

On the other hand, if the first rule is failed, the system is automatically navigated back to the homepage, and no transaction can be initiated. If the first rule checks and the second rule is flaunted, the user is notified that the requested subscription is not available for his/her type of user, the user is also given the opportunity to retry the request (Fig 4.4). However, if the user retries three more times and insists on the wrong subscription (Fig 4.5, Fig 4.6), the transaction is flagged as fraudulent and blocked automatically (Fig 4.7). The SIMcard of the user is blocked temporarily and can only be unblocked by the telecom company, after verifying the authenticity of the user who would have to provide certain legal documents before this can be implemented. These checks are important because of the losses incurred by the telecom sector as a result of users making subscription requests that are not within their service range or requesting for lower subscriptions than he should while still enjoying the quality of service that belongs to a higher user or subscriber.

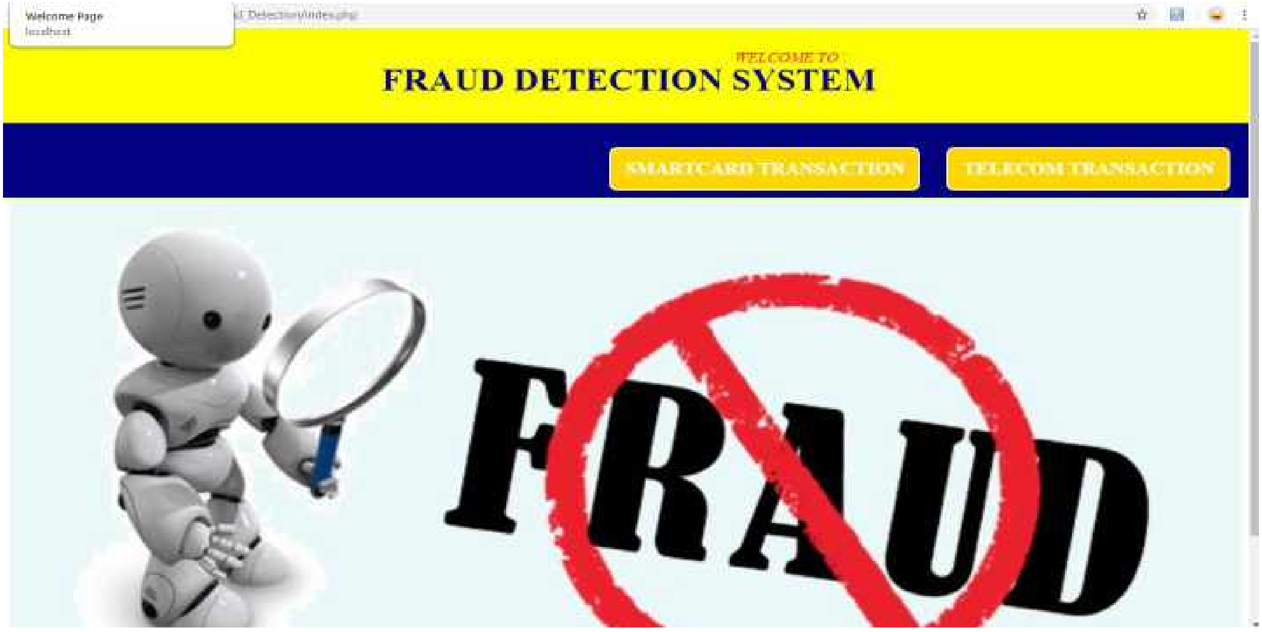


Fig.4.1: Fraud Detection Home Page

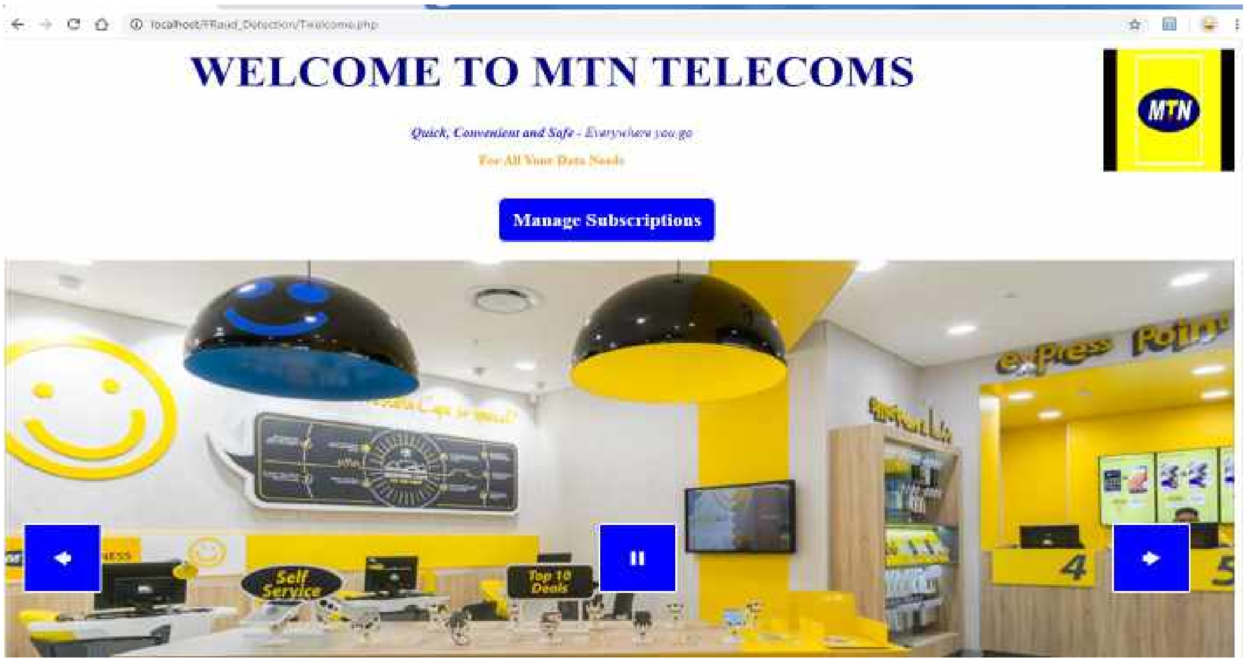
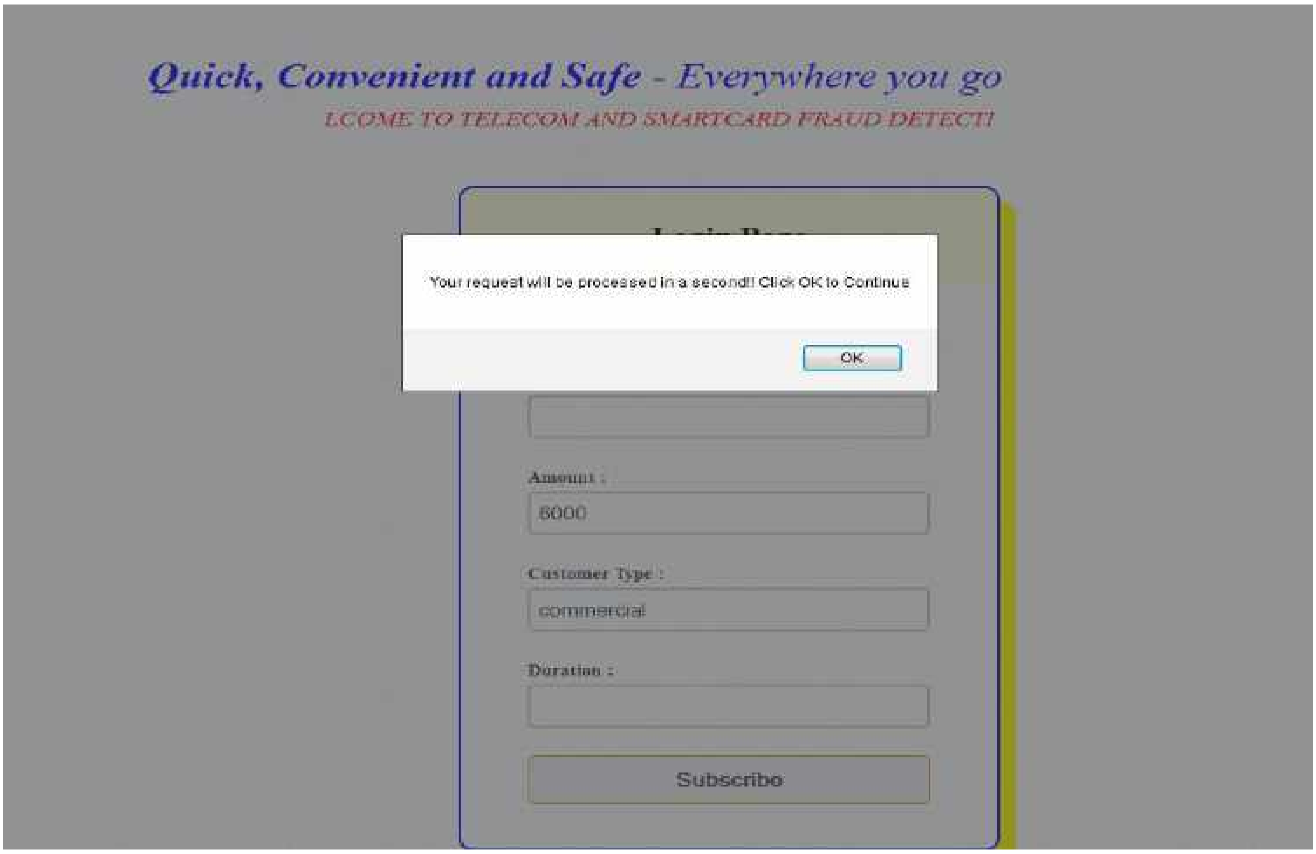


*Fig.4.2:*Telecom Welcome Page


Quick, Convenient and Safe - Everywhere you go

LCOME TO TELECOM AND SMARTCARD FRAUD DETECTI

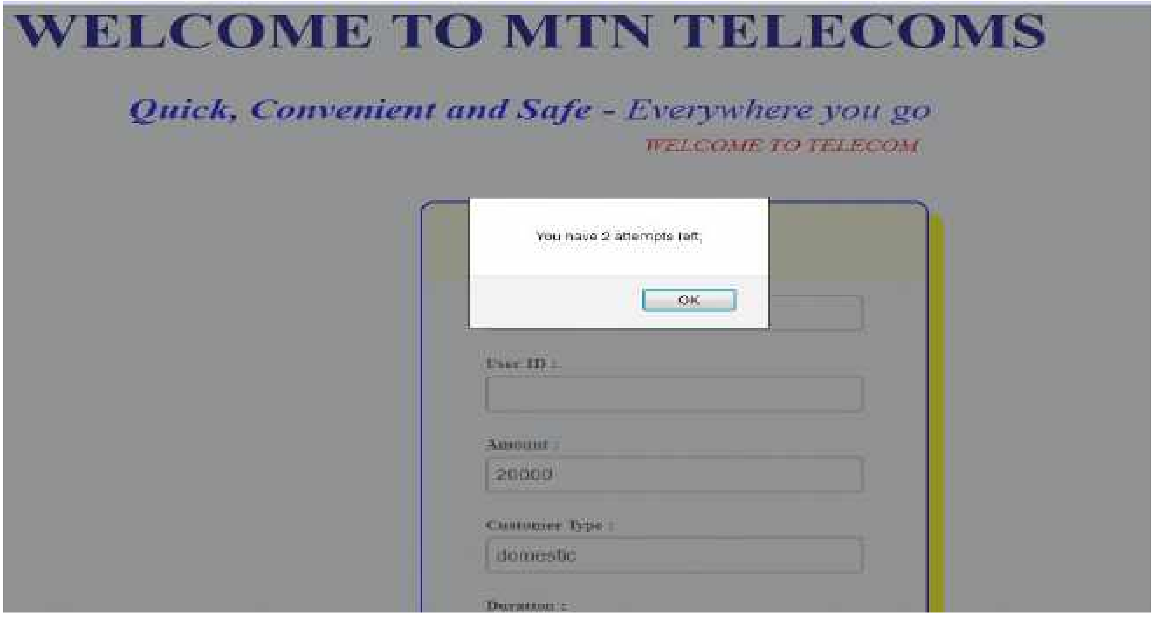
Your request will be processed in a second!! Click OK to Continue

Amount : 6000

Customer Type : commercial

Duration :

Fig.4.3: Telecom Subscription Validation Page(1)


WELCOME TO MTN TELECOMS

Quick, Convenient and Safe - Everywhere you go

WELCOME TO TELECOM

You have 2 attempts left.

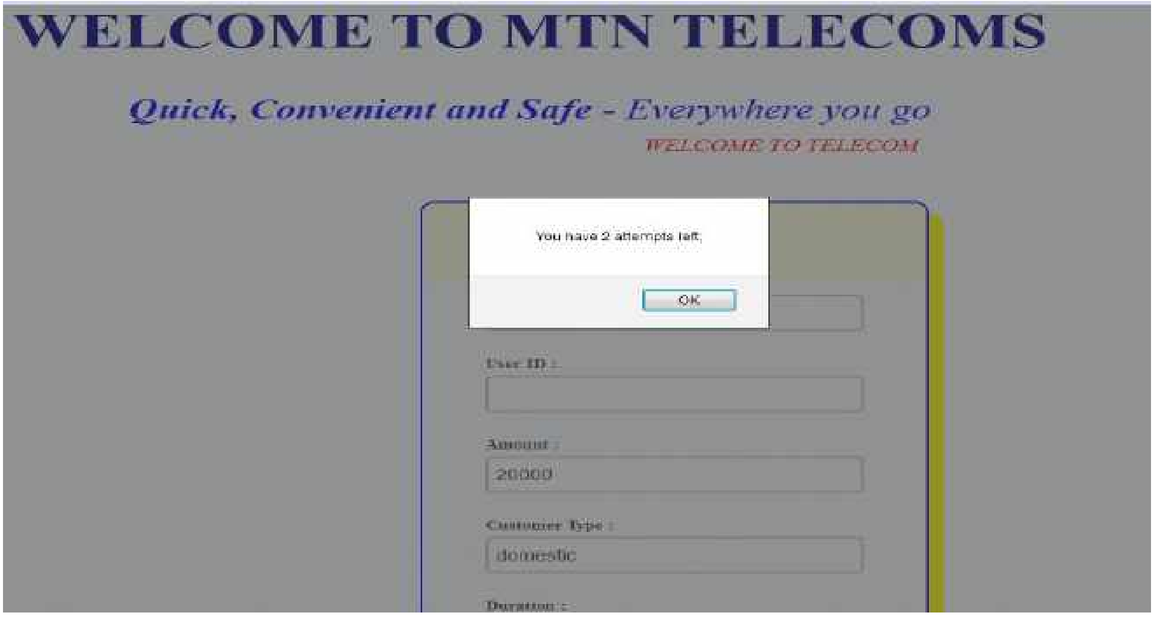
User ID :

Amount : 20000

Customer Type : domestic

Duration :

Fig.4.4: Telecom Subscription Validation Page(2)



WELCOME TO MTN TELECOMS

Quick, Convenient and Safe - Everywhere you go

WELCOME TO TELECOM

You have 2 attempts left.

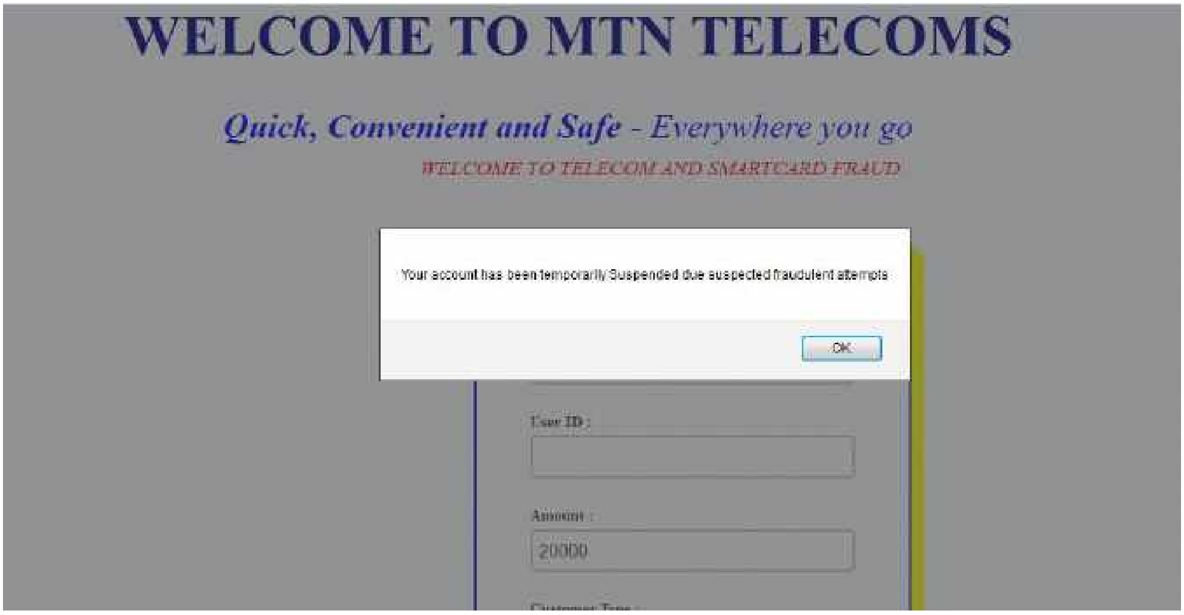
User ID :

Amount :
20000

Customer Type :
domestic

Duration :

Fig.4.5: Telecom Subscription Validation Page(3)



WELCOME TO MTN TELECOMS

Quick, Convenient and Safe - Everywhere you go

WELCOME TO TELECOM AND SMARTCARD FRAUD

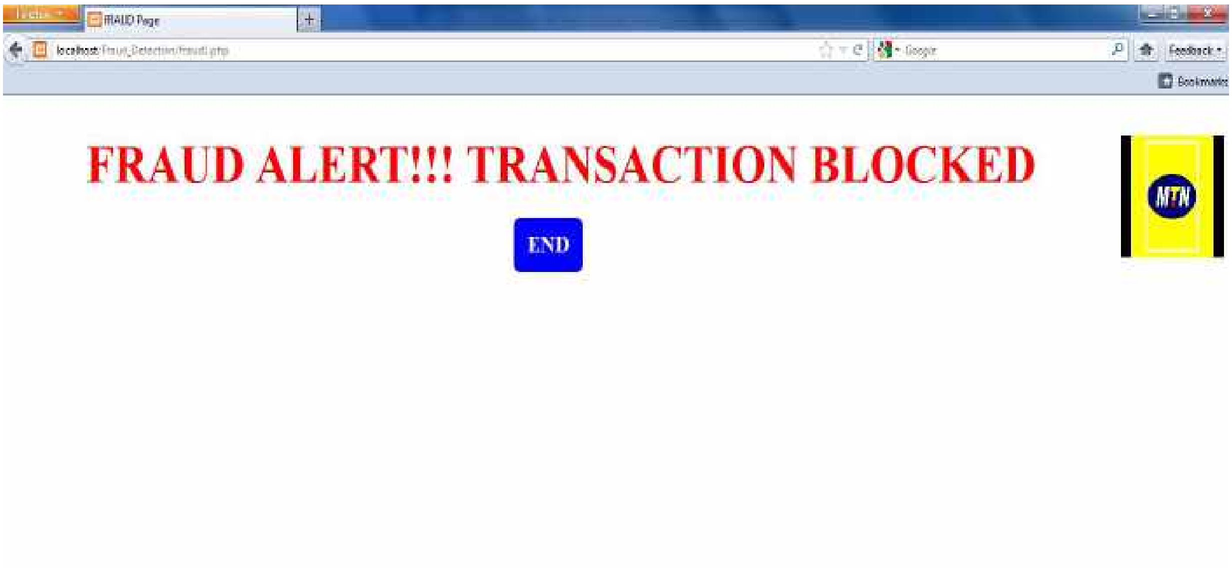
Your account has been temporarily Suspended due suspected fraudulent attempts

User ID :

Amount :
20000

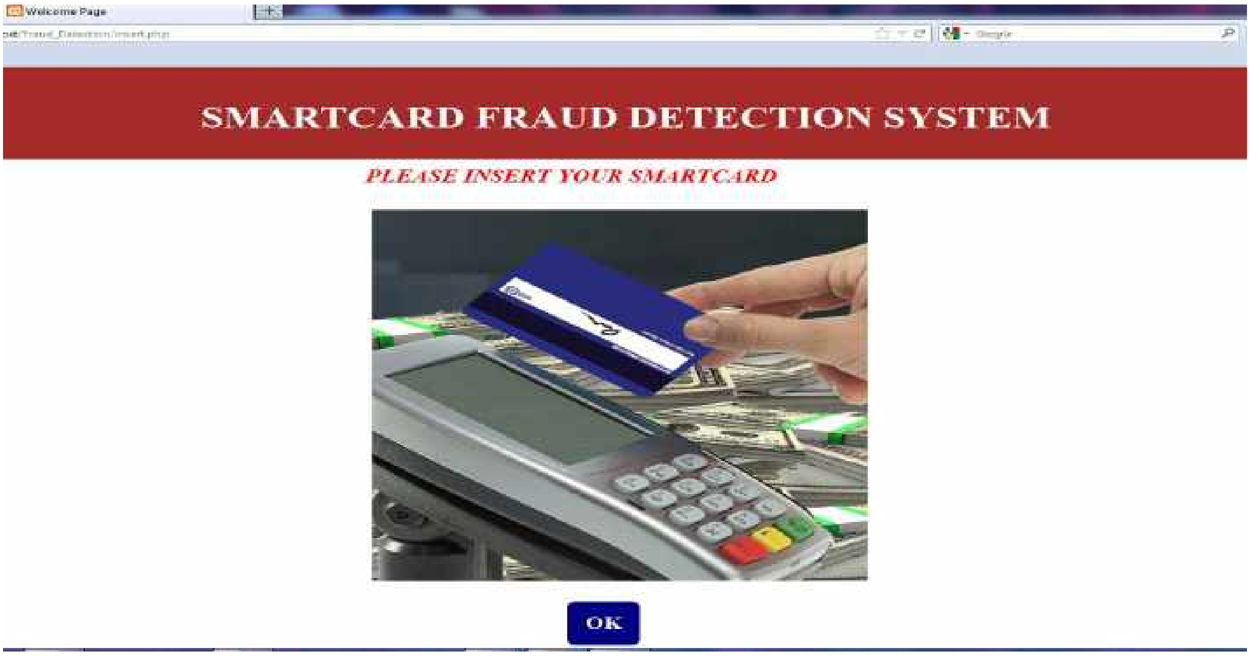
Customer Type :

Fig.4.6: Telecom Transaction Blocking Output



FRAUD ALERT!!! TRANSACTION BLOCKED

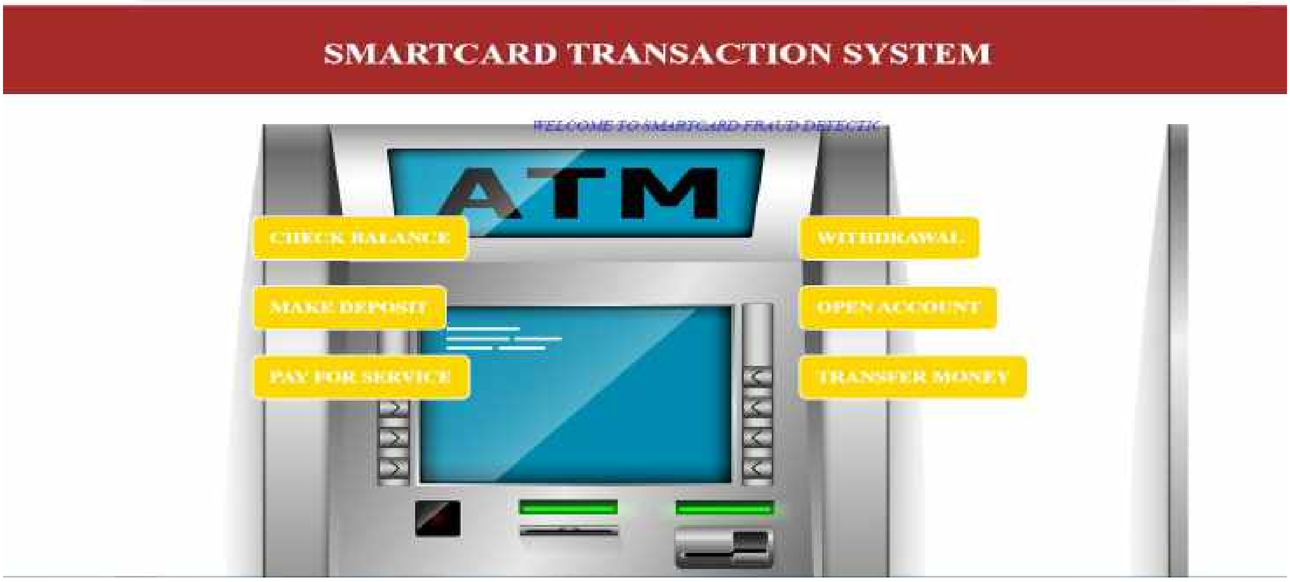
Fig.4.7: Telecom Fraud Detection Output



SMARTCARD FRAUD DETECTION SYSTEM

PLEASE INSERT YOUR SMARTCARD

Fig.4.8: Smartcard Initialization Page



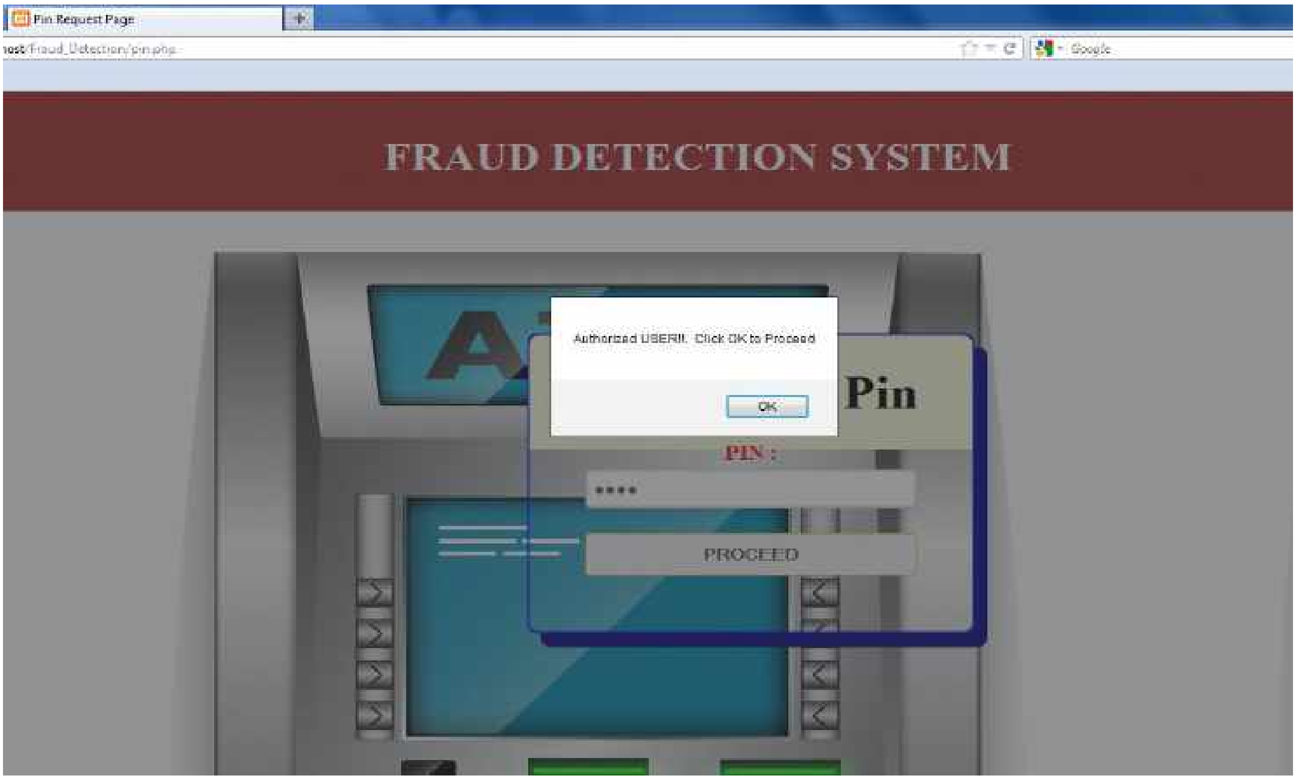
SMARTCARD TRANSACTION SYSTEM

WELCOME TO SMARTCARD FRAUD DETECTIC

Fig 4.9: Smartcard Transation Page

The smartcard transaction system as depicted in Fig 4.8, requires the use of a smartcard as the first input before any transaction can be iniatiated. Every user of the service is assumed to have pre-registered and thereby issued a smartcard to carry out certain transactions. Once the smartcard is inserted into the system: either the POS (Point of Sale) for purchase of goods and services, or the ATM (Automated Teller Machine) for withdrawal of cash and other services; the system recognizes the user and navigates him/her to the transaction page (Fig 4.9) . In this page, a list of transactions are listed out which the user can perform such as withrawal, quickmoni, transfer etc. any of the options chosen will require a secret pin from the user to perfom it. Fig 4.10 shows the output of a valid user pin. Thi means that the pin keyed in by the user is valid and the user is authentic.

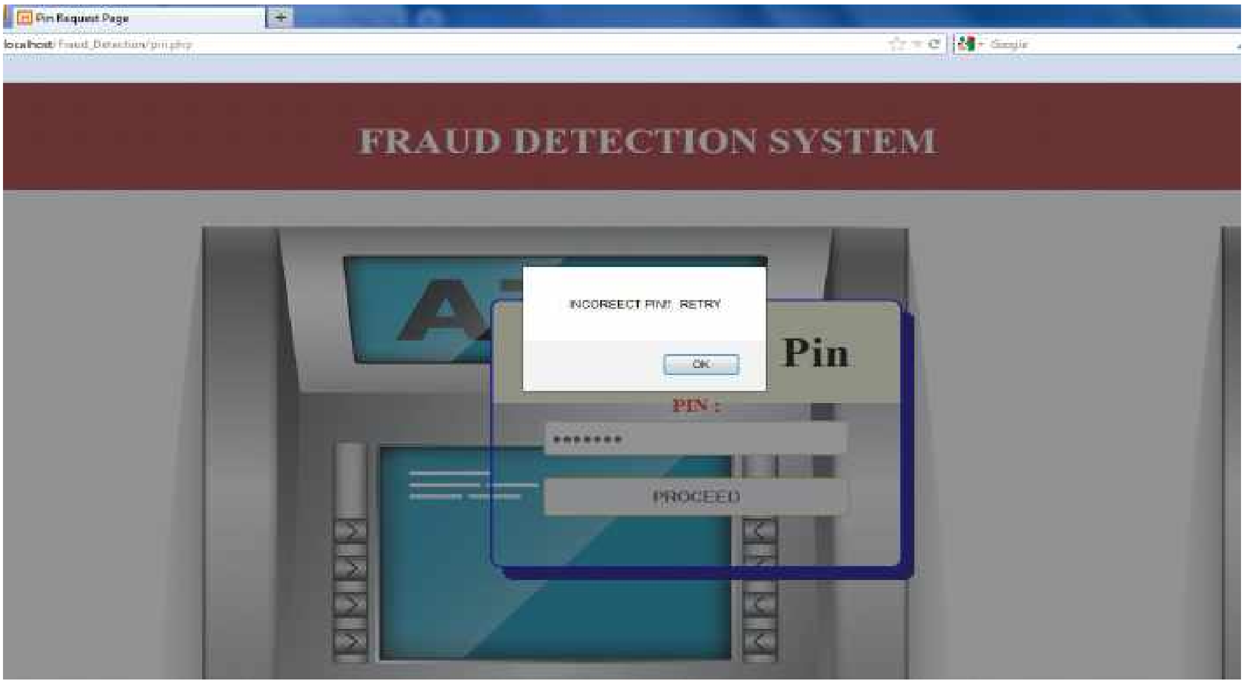
However, if the user provides an invalid pin the output in Fig 4.11 will be displayed suspending tha transaction and giving the user one more retry (Fig 4.12) and if this also fails, the user is navigated to page where the final verification is carried out to check the authenticity of the user. the user is required to provide an answer to a tricky question (Fig 4.14) which only the user can have the answer to (such as the postion of a birthmark in your body, how many birthmarks you have etc.), if this answer is correct, the uer will be given an option to reset his/her secret pin to the one they can easily remember.the user can now perform the transaction sucessfully. But if once again, the tricky question's answer provided by the user is incorrect, the transaction is automatically classifies as fraudulent and saved in the smartcard fraud database, also the transaction is blocked and flagged as frudulent (Fig 4.16) while sending an alert to the user and the financial institution about the attempted fraudulent attack



Authorized USER!!. Click OK to Proceed

PIN : ****

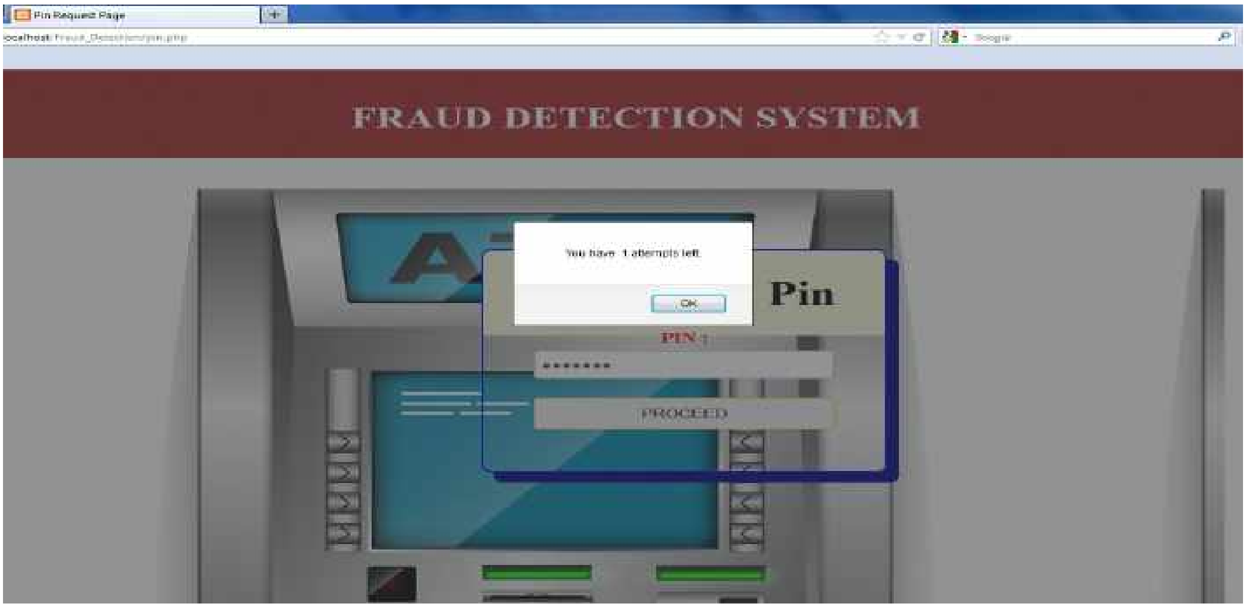
Fig 4.10: Smartcard User Validation Output(1)



INCOREECT PIN!!. RETRY

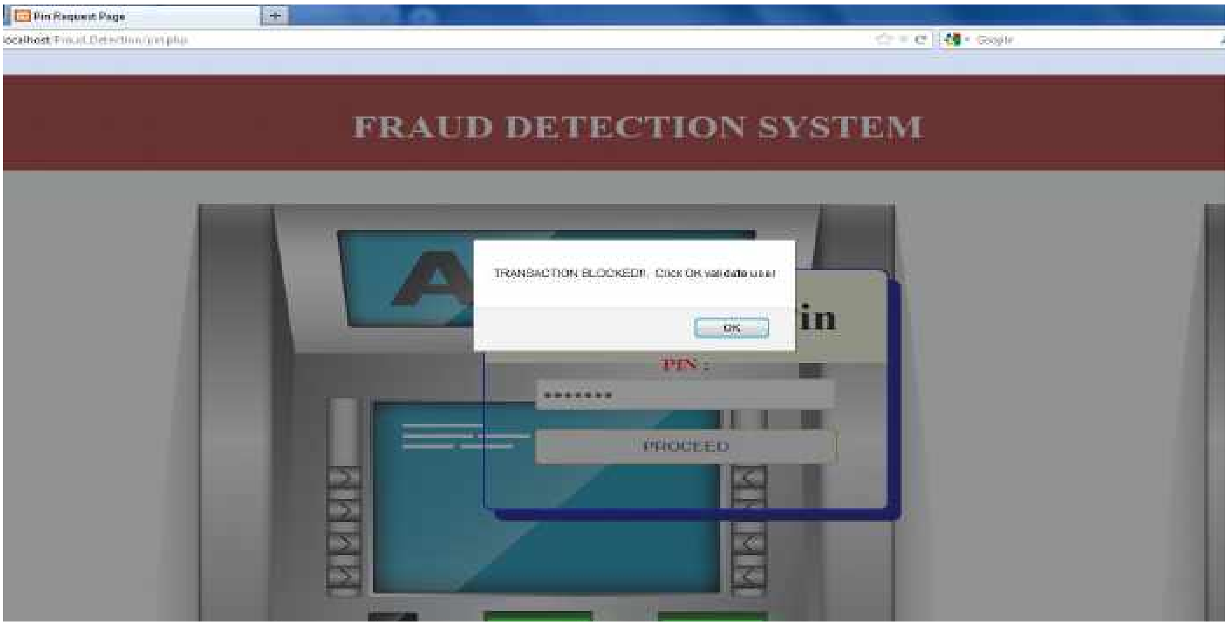
PIN : *******

Fig 4.11: Smartcard User Validation Output(2)



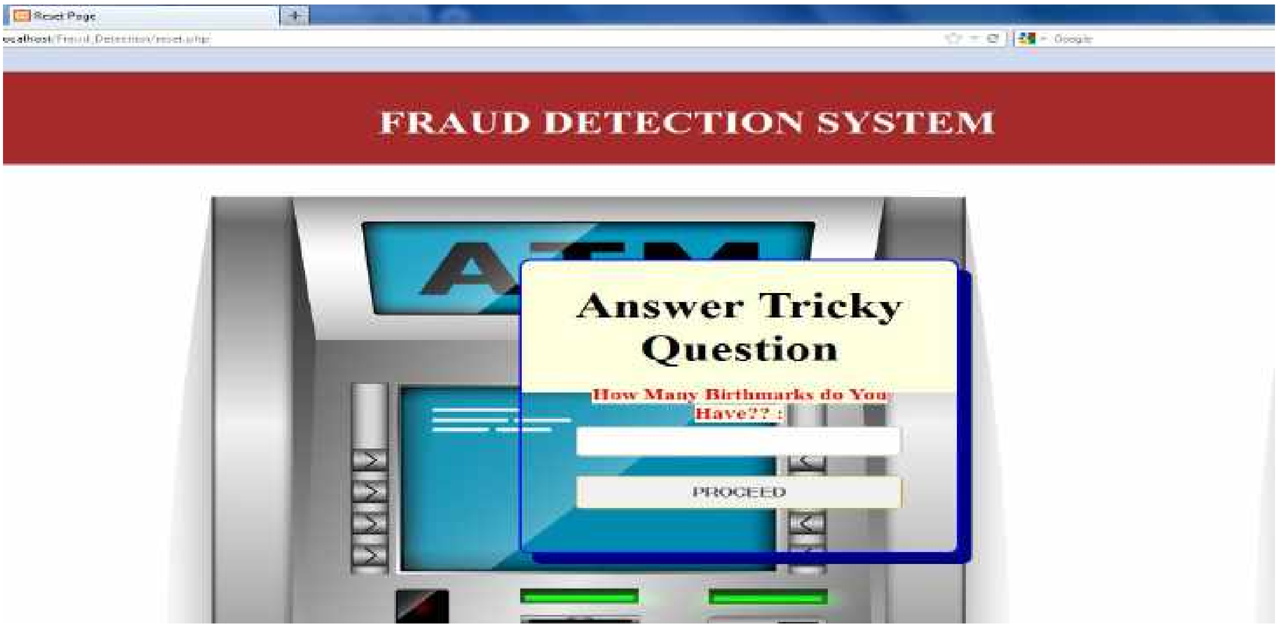
You have 1 attempts left.

Fig 4.12: Smartcard User Validation Output(3)



TRANSACTION BLOCKED!! Click OK validate user

Fig 4.13: Smartcard User Validation Output(4)

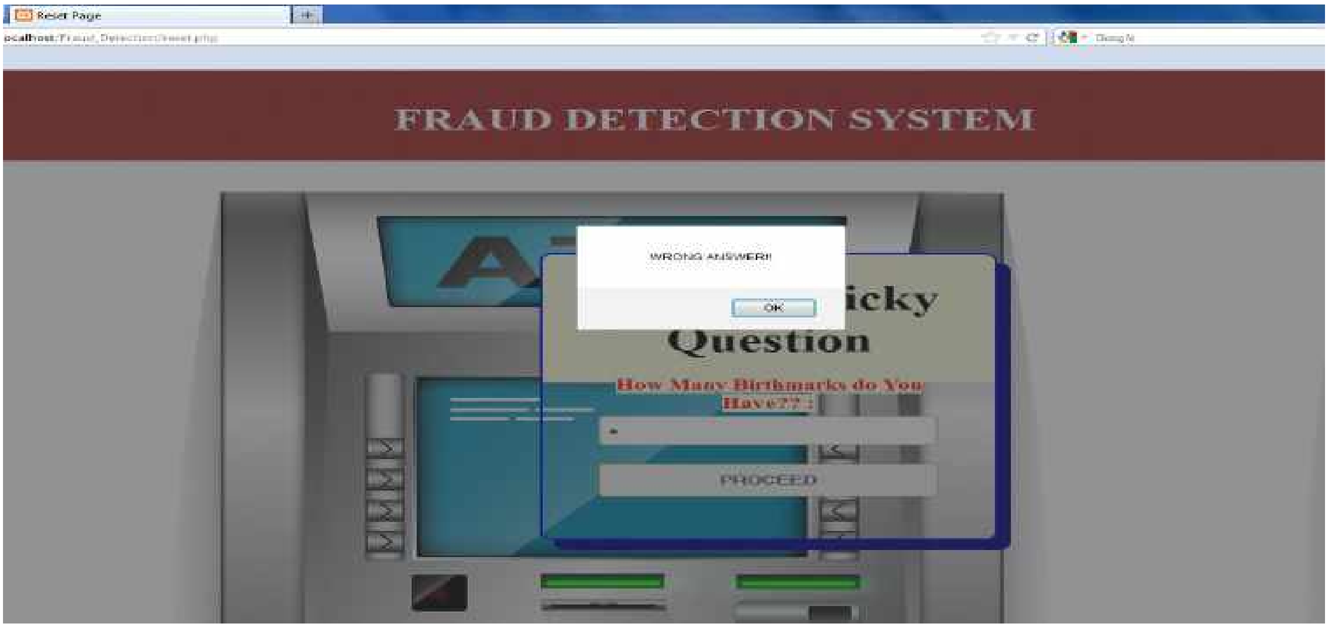


FRAUD DETECTION SYSTEM

Answer Tricky Question

How Many Birthmarks do You Have?? :

Fig 4.14: Smartcard User Pin Reset(1)



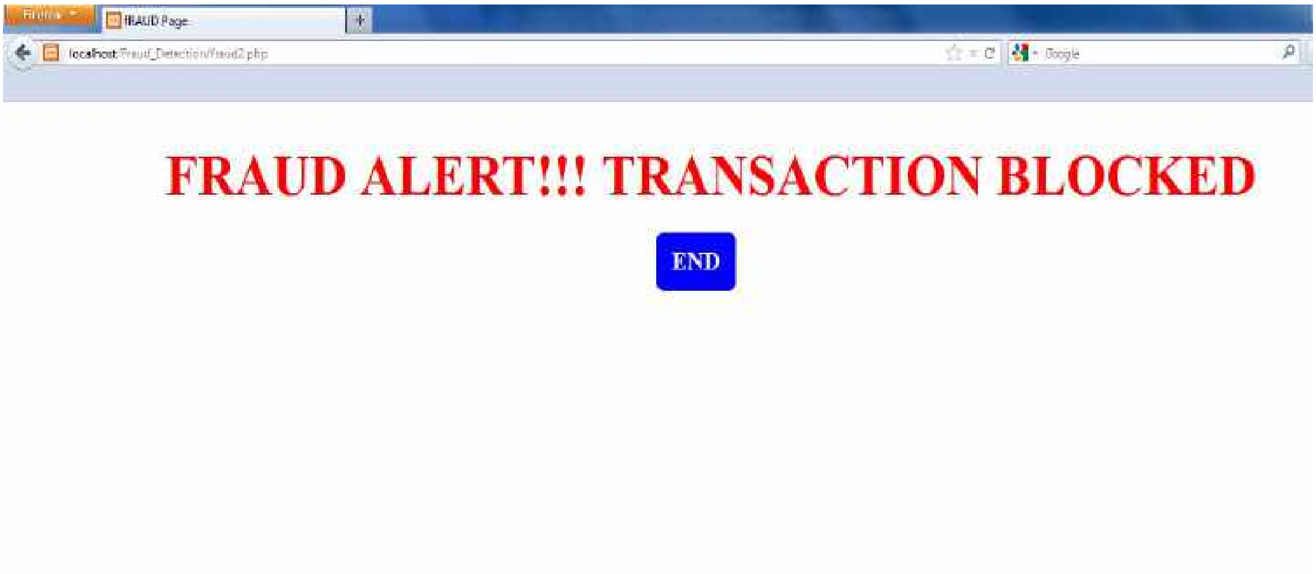
FRAUD DETECTION SYSTEM

WRONG ANSWER!!

icky Question

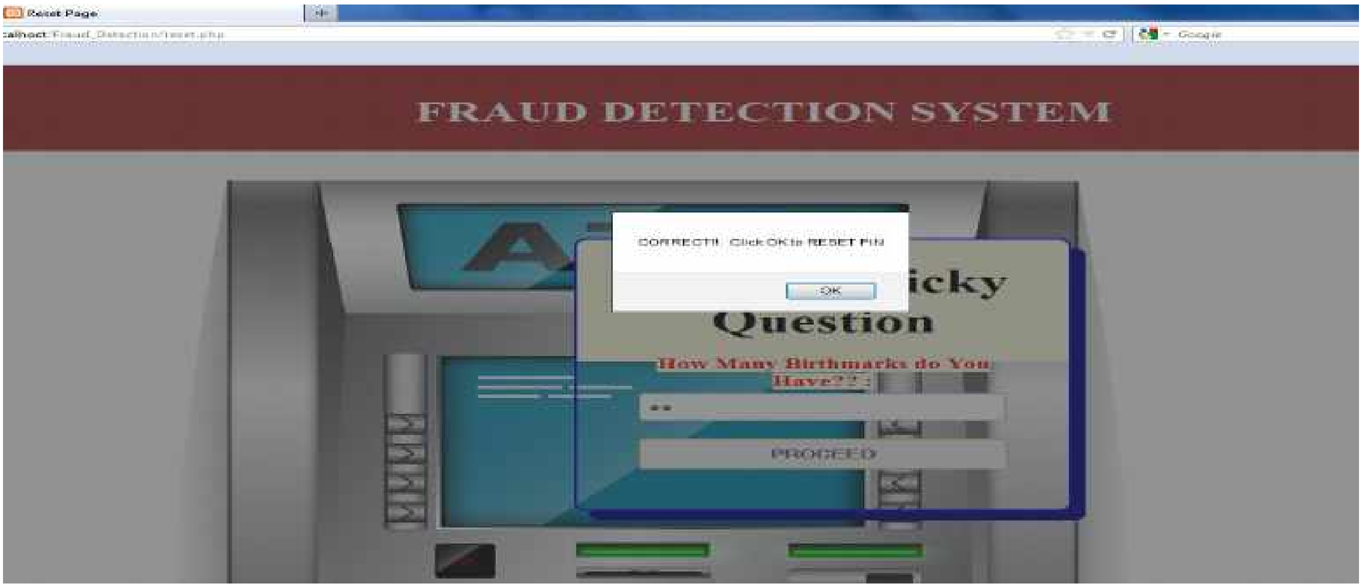
How Many Birthmarks do You Have?? :

Fig 4.15: Smartcard User Pin Reset(2)



FRAUD ALERT!!! TRANSACTION BLOCKED

Fig 4.16: Smartcard Fraud Detection Page



FRAUD DETECTION SYSTEM

CORRECT!! Click OK to RESET PIN

icky Question

How Many Birthmarks do You Have?? :

**

Fig 4.17: Smartcard User Pin Reset(3)

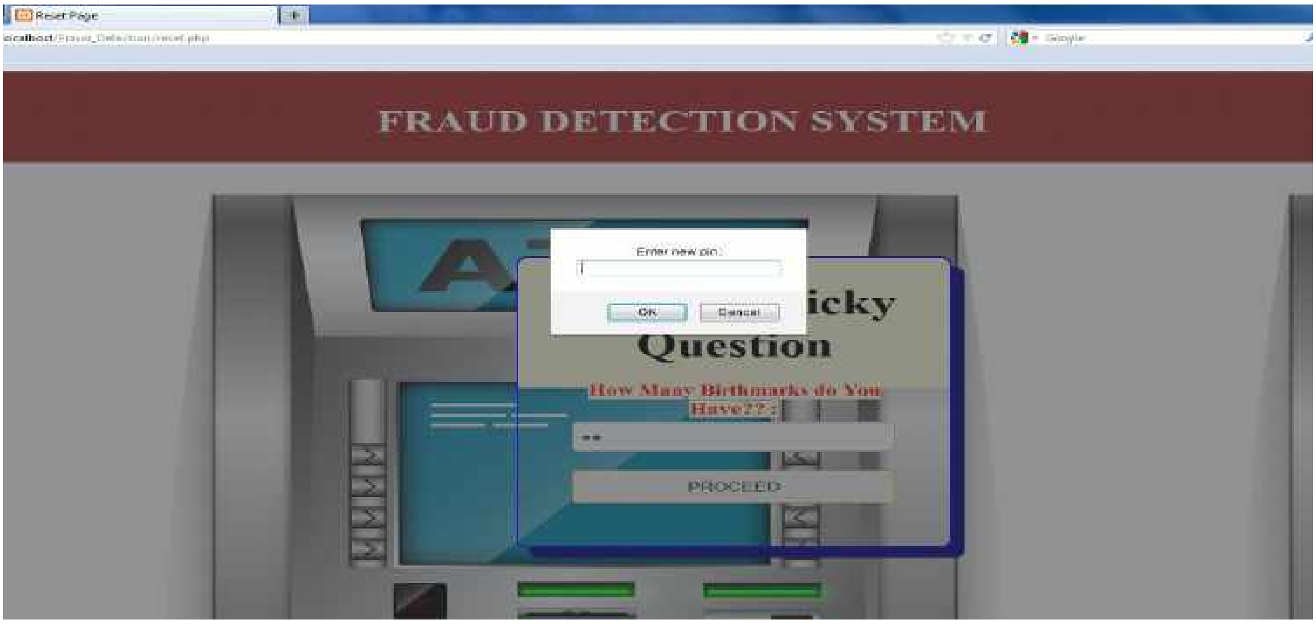


Fig 4.18: Smartcard User Pin Reset(4)

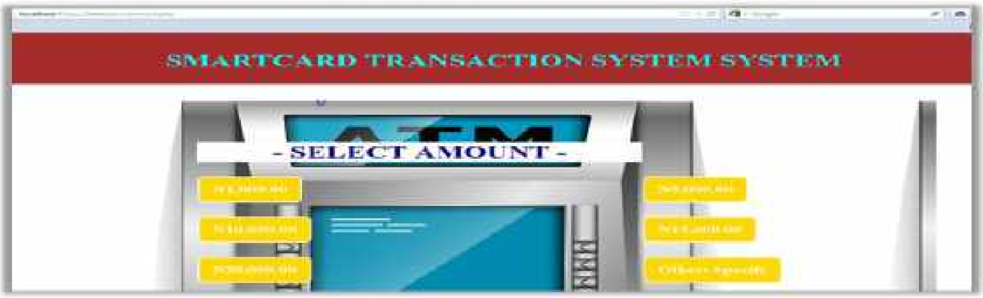
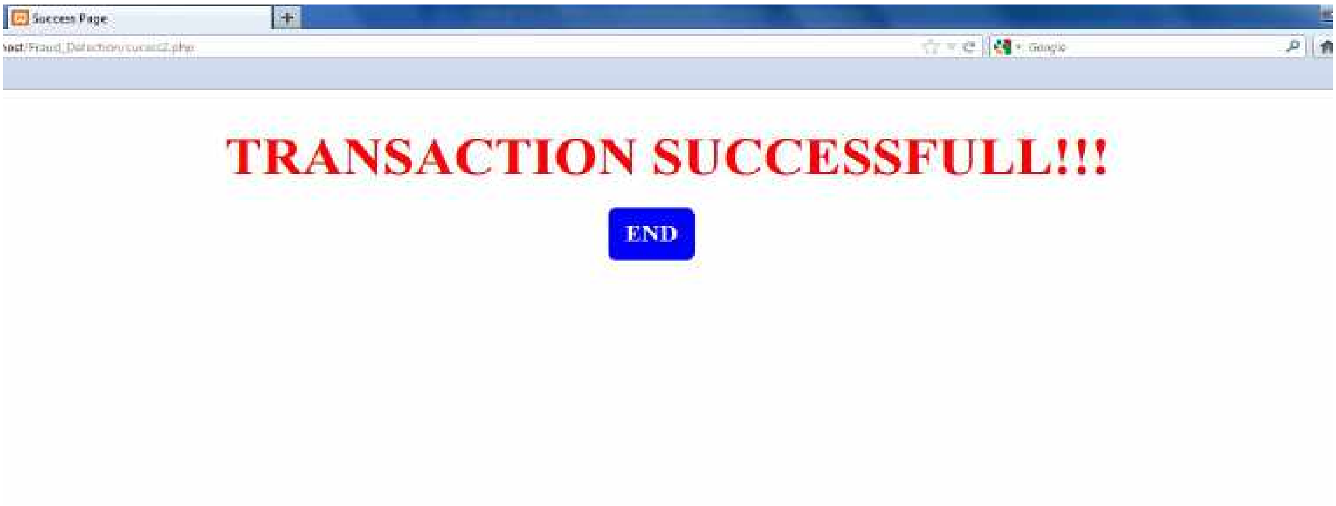


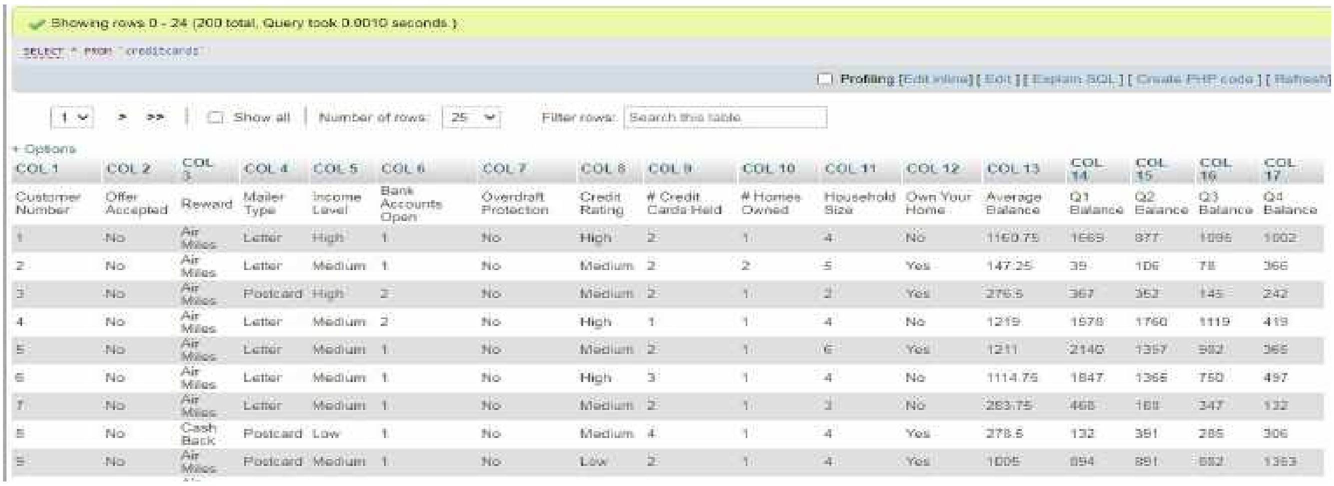
*Fig 4.19:*Select Amount Page

When compared to the existing system performance using certain parameters for evaluation, the proposed system proved more efficient an accuracy score of 94% as compared to the existing which has a score of 65%.



TRANSACTION SUCCESSFULL!!!

*Fig 4.20:*Successful Transation Page



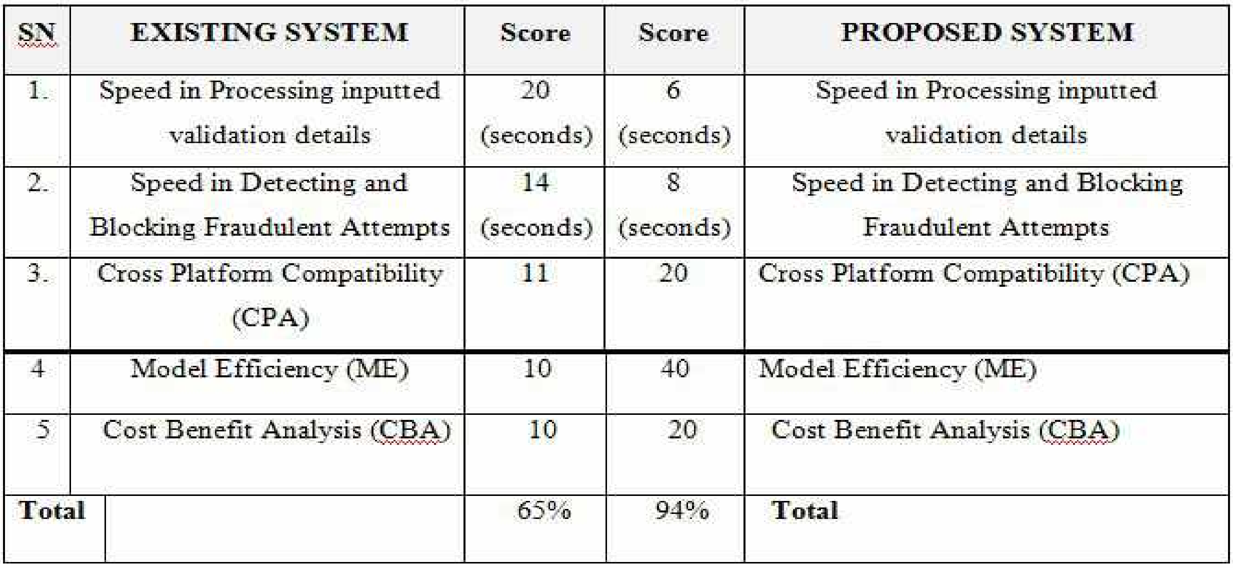
Showing rows 0 - 24 (200 total, Query took 0.0010 seconds)

```
SELECT * FROM `creditcards`
```

□ Profiling [Edit inline] [Edit] [Explain SQL] [Create PHP code] [Refresh]
1 > >> □ Show all Number of rows: 25 Filter rows: Search this table
+ Options

COL 1	COL 2	COL 3	COL 4	COL 5	COL 6	COL 7	COL 8	COL 9	COL 10	COL 11	COL 12	COL 13	COL 14	COL 15	COL 16	COL 17
Customer Number	Offer Accepted	Reward	Mailer Type	Income Level	Bank Accounts Open	Overdraft Protection	Credit Rating	# Credit Cards Held	# Homes Owned	Household Size	Own Your Home	Average Balance	Q1 Balance	Q2 Balance	Q3 Balance	Q4 Balance
1	No	Air Miles	Letter	High	1	No	High	2	1	4	No	1160.75	1669	877	1095	1002
2	No	Air Miles	Letter	Medium	1	No	Medium	2	2	5	Yes	147.25	39	106	78	366
3	No	Air Miles	Postcard	High	2	No	Medium	2	1	2	Yes	276.5	367	352	145	242
4	No	Air Miles	Letter	Medium	2	No	High	1	1	4	No	1219	1578	1760	1119	419
5	No	Air Miles	Letter	Medium	1	No	Medium	2	1	6	Yes	1211	2140	1357	982	365
6	No	Air Miles	Letter	Medium	1	No	High	3	1	4	No	1114.75	1847	1365	750	497
7	No	Air Miles	Letter	Medium	1	No	Medium	2	1	3	No	283.75	468	168	347	132
8	No	Cash Back	Postcard	Low	1	No	Medium	4	1	4	Yes	278.5	132	391	285	306
9	No	Air Miles	Postcard	Medium	1	No	Low	2	1	4	Yes	1005	894	891	882	1363

Fig 4.21: Smartcard User Table



SN	EXISTING SYSTEM	Score	Score	PROPOSED SYSTEM
1.	Speed in Processing inputted validation details	20 (seconds)	6 (seconds)	Speed in Processing inputted validation details
2.	Speed in Detecting and Blocking Fraudulent Attempts	14 (seconds)	8 (seconds)	Speed in Detecting and Blocking Fraudulent Attempts
3.	Cross Platform Compatibility (CPA)	11	20	Cross Platform Compatibility (CPA)
4	Model Efficiency (ME)	10	40	Model Efficiency (ME)
5	Cost Benefit Analysis (CBA)	10	20	Cost Benefit Analysis (CBA)
Total		65%	94%	Total

*Fig 4.22:*Comparitive Analysis

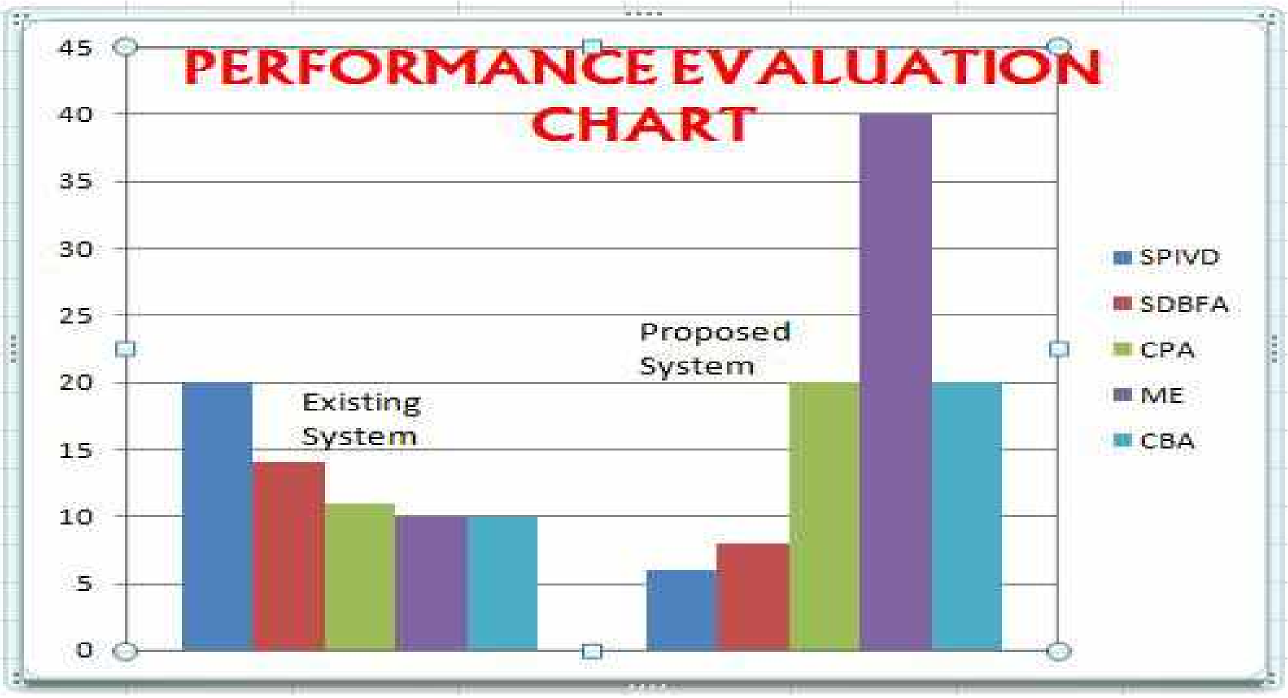


Fig 4.23: Performance Evolution Chart

V. CONCLUSION AND FUTURE WORK

This work described the development of an application for smartcard and telecommunications fraud detection. The development model involved a high security verification system to ensure that only the verified users are allowed to carry out transactions on their accounts. The security mechanisms used in classifying and detecting transactions based on the training data have been described and justified. Small parts of the developed code were presented as well as screenshots of the application.

We intend to expand the scope of the study to the development of a system that will detect other types of telecom frauds apart from the subscription fraud. Also, we intend to use a larger dataset for training the future system so that it will produce more efficient detection results. Also, we will like to introduce a hybrid model such as the neural network and the decision tree models in designing a fraud detection system.

REFERENCES

1. W.A. Oumar, and P.D. Augustin. “Credit card Detection using Artificial Neural Network,” International Journal of Innovation Technology and Exploring Engineering (IJITEE), vol.8, issue 7, pp.313-316. May 2019.
2. Z.W.W. Malek, K. Mayes, and K. Markantonakis. “Fraud Detection and Prevention in Smartcard Based Environments using Artificial Intelligence,” IFIP International Federation for Information Processing, 2008, pp. 118-132.
3. L.G. Kabari, N.D. Nanwin, and U.E. Nquoh. “Telecommunication Subscription Fraud detection using Artificial Neural Network,” Transaction on Machine Learning and Artificial Intelligence, vol.3, issue 6, pp.19-33. Dec 2015.
4. P. H. Tran, K. P. Tran, T. T. Huong, C. Heuchenne, P. HienTran, and T. M. H. Le. “Real Time Data-Driven Approaches for Credit Card Fraud Detection,” Proceedings of the 2018 International Conference on E-Business and Applications, 2018, pp. 6–9. Available: https://doi.org/10.1145/3194188.3194196
5. N. Carneiro, G. Figueira, and, M. Costa. “A Data Mining Based System for Credit-Card Fraud Detection in E-tail,”. Decision Support Systems, [Online] vol. 95, pp. 91–101. Available: *https://doi.org/10.1016/j.dss.2017.01.002. 2017*
6. Y. Jain, N. Tiwari, S. Dubey, and S. Jain. “A Comparative Analysis of Various Credit Card Fraud detection techniques,” International Journal of Recent Technology and Engineering (IJRTE), vol.7, issue 5S2, pp.402-407. Jan 2019.
7. R. Patidar, and L. Sharma. “Credit Card Fraud Detection using Neural Network,”. International Journal of Soft Computing and Engineering (IJSCE), vol.1, pp. 32–38. 2011.
8. J. Pieprzyk, H. Ghodosi, and E. Dawson.”Using Neural network for Credit Card Fraud Detection,” Information Security and Privacy, Proceedings of 12th Australasian Conference, ACISP 2007 vol. 4586. 2007.
9. A. Oodan, K. Savolaine, C. Daneshmand and P. Hoath. Telecommunications Quality of Service Management: From Legacy to Emerging Services. Let. 4(2), pp. 50-55. JUN 2003
10. M.I. Akhter, and M.G. Ahamad. “Detecting Telecommunication Fraud using Neural Networks Through Data Mining,” International Journal of Science and Engineering (IJSER), vol. 3 issue 3, pp. 1-5. MAR 2012.
11. M.J. Johnson and T.M. Khoshgoftaar. “Medicare Fraud Detection using Neural Networks,” Journal of Big Data, [Online] vol.6, issue 63, pp. 1-35. Available: *https://doi.org/10.1186/s40537-019-0225-0.*
12. S.S. Singh. “Electronic Credit Card Fraud Detection System by Collaboration of Machine Learning Models,” International Journal of Innovative Technology and Exploring Engineering (IJITEE), [Online] vol. 8, issue 12S, pp. 92-94. OCT 2019. Available: DOI:10.35940/ijitee.L1028.10812S19.
13. B.C. Amanze, and C.G. Onukwugha. “Credit Card Fraud Detection System in Nigeria Banks

using Adaptive Data Mining and Intelligent Agents: A Review," International Journal of Scientific Technology Research, vol. 7, issue 7, pp. 175-184. JUL 2018

14. B.C. Amanze, D.C. Asogwa, and C.I. Chukwuneke. "Credit Card Fraud Detection System using Intelligent Agents and Enhanced Security Features," International Journal of Trend in Research and Development (IJTRD), vol. 5, issue 3, pp. 524-530. MAY 2018.
15. S. Daliri. "Using Harmony Search Algorithm in Neural Network to Improve Fraud Detection in the Banking System," Computational Intelligence and Neuroscience, [Online] vol. 2020, pp. 1-5. Available: *https://doi.org/10.1155/2020/6503459.*
16. L. Delamire, H. Abdou, and J. Pointon. "Credit Card Fraud Detection Techniques: A Review," Banks and Banks System¸ vol. 4, issue 2, pp. 57-68. JAN 2009.
17. M. Zanin, M. Romance, S. Moral, and R. Criado. "Credit Card Fraud Detection through Parenclitic Network Analysis," Hihawi Complexity, [Online] pp. 1-9. Available: *https://doi.org/10.1155/2018/5764370. MAY 2018*
18. Z. Zhang, X. Zhou, X. Zhang, L. Wang, and P. Wang. "A Model Based on Convolutionary Neural Network for Online Transaction Fraud Detection," Hindawi Security and Communication Networks, [Online] pp. 1-9. Available: *https://doi.org/10.1155/2018/5680264.*
19. I. Sadgali, N. Sael. and F. Benabbou. "Fraud Detection in Credit Card Transaction using NeuralNetworks,' SAC2019, Casablanca, Morocco, 2019, pp. 1-4. Available: *https://doi.org/10.1145/3368756.3369082.*
20. Y. Abakarim, M. Lahhby, and A. Attioui. "An Efficient Real Time Model for Credit Card Fraud detection Based on Deep Learning," 12th International Conference on nIntelligent Systems: Theories and Application (STA'18), Rabat, Morocco, 2018, pp. 1-7, Available: *https://doi.org/10.1145/3289402.3289530.*

This page is intentionally left blank