International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 3 Mar 2022, pp: 386-393 www.ijaem.net ISSN: 2395-5252

Fraud Reduction in Electronic Card Payment System Using Hybrid Model and Enhanced Security Features

Amaefule I.A[#1], Chilaka U.L[*2,] Ibebuogu C.C[#3]
[#1 & #3] *Department of Computer Science Imo State University, Owerri. Imo State, Nigeria*
[*2] *Department of Computer Science, Federal Polytechnic Nekede, Owerri. Imo State, Nigeria*

Submitted: 01-03-2022 Revised: 10-03-2022 Accepted: 12-03-2022

ABSTRACT
The popularity of credit card for purchases of goods and services tends not to diminish because of its ease of use and convenience. However, the rate of fraudulent activities connected with the integration of electronic payment has expanded. To minimize unwanted activities of fraudster, efficient timely method assurance of fraud detection capability of credit card payment system must be established. The purpose of this work is to develop a security system that will promote trust in communication channels using Hidden Markov model (HMM) and Neural Network (NN) that could combine proofs from current and legitimate regular activities of the credit-card owner for the past one or two years on its credit-card to ascertain suspicious level of every transaction. The system developed is an online tool which used Hybrid approach to detect, control and monitor fraud in electronic payment. The outcomes express that hybrid approach performances considerably reduce fraud loss.

Keywords: Electronic payment, internal control, electronic fraud, security system, fraud detection.

I. INTRODUTION:

The emerging technologies have expanded opportunities for the criminal element and cybercrime; these developments tend not to reduce, due to rapid increment by legitimate customer in the usage of electronic payment. However, the fixed integration of e-commerce has exposed businesses to a wide range of threats such as security, privacy and reliability apprehensions [1]. Real and perceived security apprehensions in particular, are barriers preventing a more rapid update and growth of e-commerce [2].

Appropriate acknowledgment of payment in exchange for goods and services is what company and client look forward to; in any transaction indication of fraud occurrence may be perceived if one party fails to receive what they anticipate. Financial agencies are looking for the acceleration and speedy recognition of activities of fraudsters and swindlers, in order to stop them before they can harm customers and financial institutions.

Combating virtual fraud is very complicated task in a faceless world, and any response designed to counter it must be capable of doing so in a timely fashion. The actuality of fraud or still the risk of it, is major a barrier preventing users in performing transactions [2]. It is evident that businesses will benefit greatly from efficient fraud detection method but the development of those controls is also vital for financial institutions.

Fraud Techniques

Fraudsters execute credit card fraud through many channels; as new technology emerges also are more opportunities for fraudsters to commit fraud. Different methods of committing credit card fraud are explained below.

A. **Dealer (Merchant) Related fraud:** Dealer related frauds commences either by proprietors of the dealer organization or their workers. These kinds of frauds kicked off by dealer are described below: [3].

1. **Merchant Collusion:** This form of fraud happens when business dealers or their workers connive to commit fraud with the card owner accounts or with the individual Information, They provide card owners details to the fraudsters.

2. **Triangulation:** Triangulation is a form of fraud which happens over the internet (web site). The supplies or commodities are presented at greatly reduced price and as well sent before imbursement. The client while surfing the website and if he needs the commodities he put the online details such as person's name, delivery address and actual credit card information to the website. When the impostors collect these particulars, they arrange commodities from a genuine website with this pilfer credit card information.

B. **Web (Internet) Related Frauds:** Web is the foundation for the impostors to commit their defrauding in an easy and an effortless method. Fraudsters have lately started to function on an actual international stage. The major frequently employed methods in web (Internet) fraud are explained below [3].

1. **Site cloning:** Site cloning is a procedure where an impostors clone a whole website from which the client purchased items, clients have no cause to think they are not relating with the corporation that they desired to purchase commodities from, since the sites they are seeing look alike to the genuine website.

2. **False merchant sites:** Several websites frequently present low-priced products to the consumers. With the objective to ask for the consumer for total form information which includes address and name to gain entry to the website where the consumer obtains his desired goods. A lot of these websites maintain to be free of charge, but need an authentic credit card number to verify an individual's birth date.

3. **Credit card generators:** They are software programs that generate numerically valid credit card numbers and expiration dates. These software works by generating random records of credit card numbers from a solitary number.

C. Card Related Fraud

1. **Fraudulent application**: - when an impostor make use of another individual's details and name to request for and acquire a card.
2. **Lost/Stolen Cards:** When an individual loses his credit card or the credit card is pilfered by fraudster or when a genuine cardholder takes delivery of a credit card and misplaces it or fraudster pilfers the card for illegal reasons.
3. **Account Takeover:** This category of fraud happens when the legitimate cardholder's private detail is stolen by swindlers. The impostor acquires control of a valid account by make available the client's account digits or the credit card digits. The impostors then reach with the cardholder bank, as he genuine cardholder, to ask the mail to redirect to a new address. The fraudster reports card lost and asks for a replacement to be sent [3].
4. **Fake and Counterfeit Cards:** This is a different fraud type where the generating of forged credit cards, jointly by stolen or misplaced cards creates maximum risk in card frauds. Fraudsters are frequently discovering a fresh and more advanced means to generate counterfeit cards. The below mentioned are few mechanisms employed for making forged and counterfeit cards: [3].

i) **Erasing the magnetic strip:** This is fraud type where the impostors expunge the magnetic strip by via potent electro-magnet, The impostor then interferes with the information on the credit card so as to match the information on a legitimate card, which they could possibly reached

ii) **Creating a Counterfeit or Fake Card:** Presently, we have urbane devices where an individual can make a counterfeit card from the beginning. This is an ordinary fraud although a counterfeit card entails much effort and skillfulness to create it. However, cards we have today has lots of security trait, all intended to ensure it difficult for an impostors to carry out fraudulent activities. It's extremely difficult to falsify credit cards successfully following the introduction of Holograms in it

iii) **Skimming:** Skimming is rapidly becoming the trendiest type of fraud in credit card transact. Most instances of counterfeit fraud employ skimming. It is a process where the real data on a credit card's magnetic strip is by electronic means duplicate into another card.

iv) **White Plastic:** White plastic is same like credit cards which the color vary, that a impostor produces and programs with valid magnetic strip records for illegitimate transactions. The fraudsters use this at POS terminals for this they don't require card validation or verification.

II. LITERATURE REVIEW

[4]**;** A fraud density map method was presented by Kim, to advance the learning

competence of a neural network. However, an over-stress of falsified transactions in data sets training was observed; thus the disjointed distributions concern of genuine and illegitimate transactions involving the data training and actual data was handled by (FDM) fraud density map. FDM adjusts the bias found in the data training by reflecting the distribution of the real data onto the training data through the changing of a weighted fraud score. They system has some Limitations which includes; problem of number of parameter - has to be put in place prior to the beginning of any training, the training outcome can be nondeterministic and depend crucially on the choice of initial parameters and lack of methods exists to ascertain the finest topology for a specified problem due to its high complexity of large networks.

[5]**;** Identified the problem of credit card transaction data having a natural skewness towards legitimate transactions; the ratio of fraud transactions to normal transactions is extremely low for an individual FI, and this makes it difficult for FIs to maintain updated fraud patterns. The authors of this thesis proposed web service techniques for FIs to share their individual fraud transactions to a centralized data center and a rule-based data mining algorithm was then applied to the combined dataset to detect credit card fraud. However, their limitations are difficult to maintain updated fraud pattern, extreme sensitive to noise and their performance deteriorates rapidly in the presence of spurious data.

[6]**;** suggested an unsupervised discovery technique of credit card by monitoring irregular spending activities behavior and transactions incidence. The mean sum spent over a particular time frame was employed as the contrast guide. However, Bolton and Hand presented (PGA) Peer Group Analysis and (BPA) Break Point Analysis methods as unsupervised outlier discovery systems. The result revealed that the PGA method is capable of effective detection of local irregularity in the records, and the BPA method is effective in concluding fraudulent activities by putting side by side transactions at the launch and close of a specified period. Main Limitations encountered is Complexity and inability to recover from database corruption, non numerical data need to be converted and normalized and Sensitivity to data format.

[7]**;** Studied particularly at credit card transaction scam and detected fraud instances by employing a two approach of neural network algorithm with rule-based classification method. In this procedure the rule-base classifier initially verified weather a transaction was falsified, subsequently the dealing classifications were confirmed by a neural network. However, this method raises the chances for analysis of fraud to be accurate and consequently, capable of reducing the quantity of false alerts while growing the assurance level. Its major setback is difficult to handle missing data, over-fitting problem and poor explanation capability

Algorithm Used

```
Given: Transaction Model T(S, S')
    Sensing Model S(S, O)
    Observations $O_1$, …………… $O_T$
Find: Most probable $S_1$, ……………, $S_T$
Initialize S x T matrix V with Os
$V_{0,0} \leftarrow 1$
For each time t = 0 to T – 1
    For each state S
        For each new state S'
            Score $\leftarrow$ Vs,t * T(S,S') * S(S',Ot)
                If score = 0 and > 0,
                    Generate codes
                Else
                    Back from S with Max $Vs_{,T}$
                End if
        End For
    End For
End For
End
```

Neural Network: after successful generation of confirmation code, other input layer such as email id and phone number, security question, amount of transaction together with the customer PIN are integrated in the hidden layer to form the output layer. Figure 1 show the Neural Network approach.

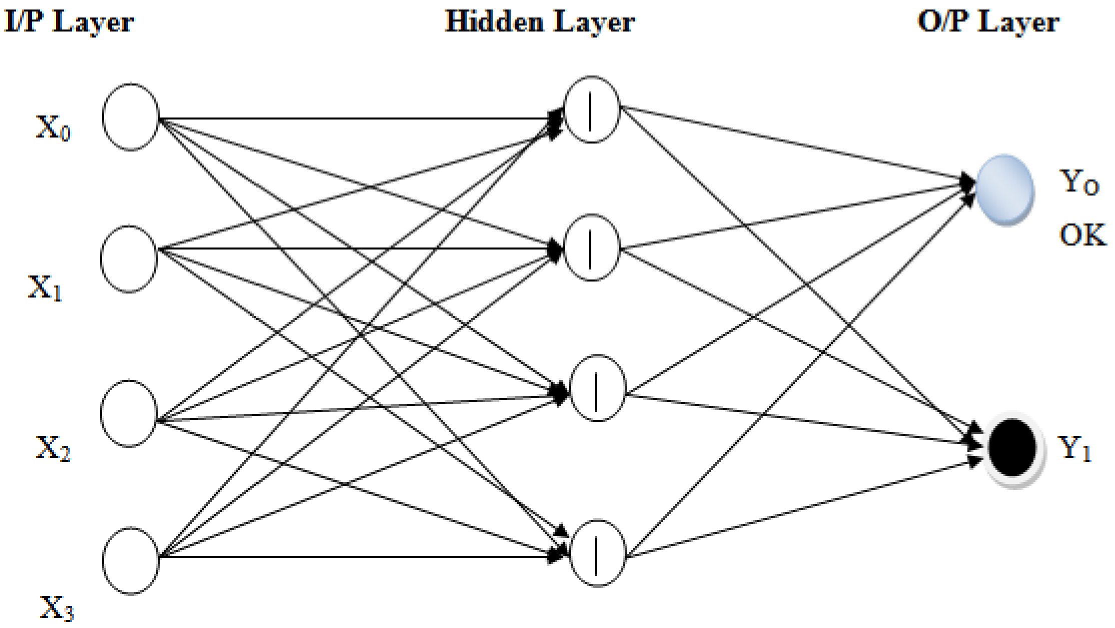


Figure 1: Neural Network of Fraud Discovery Structure

X_0, X_1, X_2 and X_3 are the input neurons which generated as follows

X_0 = Confirmation code
X_1 = Email id and phone number
X_2 = Security Question
X_3 = Amount of transaction

These input neuron are integrated in the hidden layer to form output layer Y_0 or Y_1

Y_0 = Successful integration of input neurons

Y_1 = Unsuccessful integration of input neurons

Analysis of the New System

The proposed system has three (3) data engine which are Customer Database, Bank Database and Fraud Database, each of these databases has its specific functions in Fraud Discovery Structure (FDS).

The Customer Database; stores the activities of the user like new account opened by the customer, all transactions made both deposit and withdrawal, view past transaction, account balance, account edit and update are all kept in the customer database.

The Bank Database; where all the administrator activities are stored such as configuring and maintaining various variable in the system like open new account, block/unblock account, trace fraud, transaction declined, customer care and all administrative access right to each module in the system are contained in the database; also creating/restricting access to user profile. Equally all genuine transactions that have passed the authentication checks are also stored in the bank database. However, since the new system will be embedded in the existing system, the authentication check will retrieve its information from legitimate regular activities of the credit-card owner for the past one or two years on its credit-card stored in the existing bank database.

Fraud Database stores all suspicious attempt made to the customer account; and other transactions that failed the authentication check are automatically send to fraud database for further investigation regarding the fraudulent transaction.

The new FDS will confirm every detail about the credit card information (like credit card number, type, CVV number, expiration month and year of the card etc.) with credit card customer database. If the information entered is correct, then it will request for Personal Identification Number (PIN), after matching the PIN with the database as well as account balance, the fraud authentication check will be activated.

The new Fraud Discovery System is built on a hybrid approach of Hidden Markov Model (HMM) and Neural Network (NN). The HMM will be used to generate the confirmation code, email id, phone number, security questions and also amount of transaction. The Neural Network technology receives its input from HMM authenticates these parameters about the particular pattern of using a credit card by a particular cardholder.

In spite of behavior of credit card use, neural network is as well trained as regards to the different credit card fraud features by a particular financial institution earlier. From the behavior of applications usage of credit card, neural network employ prediction algorithm on card owner data behavior to classify whether the transaction is legitimate or not. If the pattern are matched, the transaction will be declare okay by neural network, it stores it in the bank database and consider it in future for reference; if the pattern differs from the past transactions, the system concludes that it is unauthorized user access and generates an alert message to the valid user and admin and the fraudster details and location through internet protocol (IP) address will automatically sent and stored in the fraud database for further investigation. The issuing bank regrets the transaction and blocks the account temporarily.

This system will be embedded in the present electronic card verification system to enhance security and reduce external fraud. However, it is significant to note; in this new model every state is fully connected with the hybrid technology of Hidden Markov model and Neural Network which can easily be reached just in a single step; this scalability forms the optimum consideration as summarized architecture is shown in figure 2.

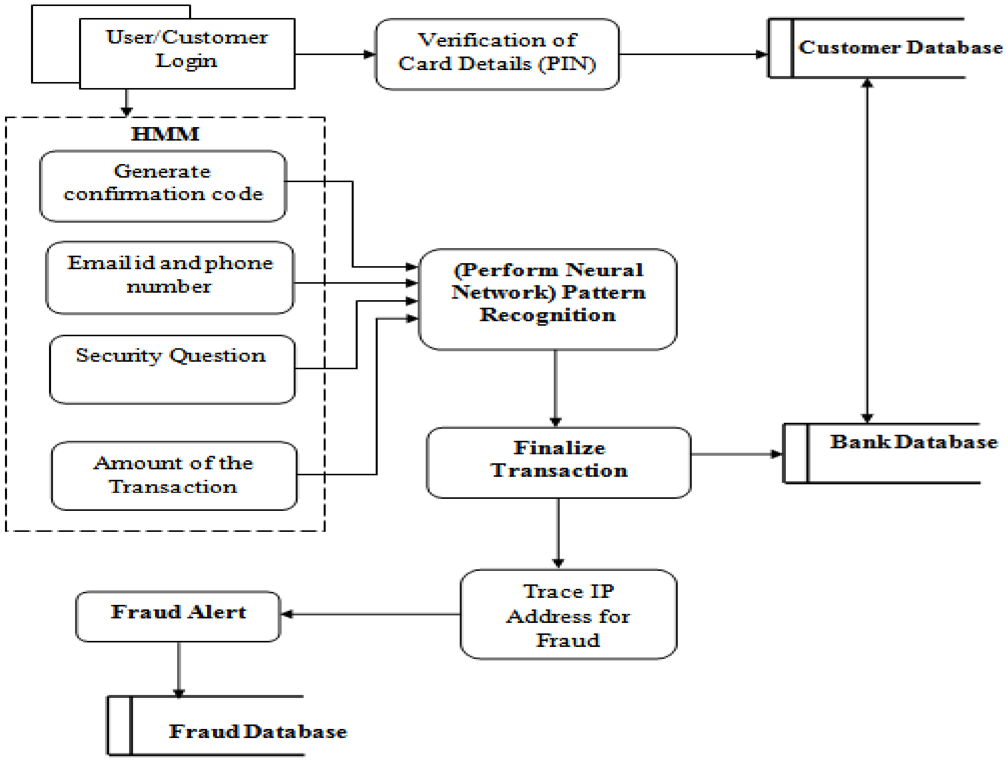

User/Customer Login
Verification of Card Details (PIN)
Customer Database
HMM
Generate confirmation code
Email id and phone number
Security Question
Amount of the Transaction
(Perform Neural Network) Pattern Recognition
Finalize Transaction
Bank Database
Trace IP Address for Fraud
Fraud Alert
Fraud Database

Figure 2: Dataflow diagram of the New Fraud Detection System.

Additional Security Features

With the progressive motion of the hybrid method algorithm for fraud discovery, we have applied more features such as security question; confirmation code, shipping location details and internet protocol address are all established and verified for further security. These information are provided during the time of registration the by customer and saved in the database for future verification reference. It will verify the secret security questions, shipping location details and the IP address each time the customer is making a transaction for enhanced security, verification and confirmation purposes. If any abnormality is discovered, then it will activate the fraud discovery system and essential measures are taken to guarantee the customer is genuine; equally the confirmation code is sent the phone number of the client to verify and authenticate the customer carrying out the transaction.

Merit of the New System

The new system will be of huge advantage to the financial establishments and its customer; which includes:

1. The customer detail and activity log is maintained, and will be utilized as evidence by the financial establishments for the transaction performed by the customer.

2. The hybrid structure will establish a more secured communication controls for the user transactions thus prevent loss of funds by the user to fraudsters.

3. The hybrid technology system guarantees that every sensitive data (for instance credit card number etc) are encrypted and access to data in its totality are only for approved users.

4. Improve alert quality and accuracy; the new system is featured with alert system to enable card owners receive alert of fraudulent activities and automatically disable customer's (victims) account involved.

New System Justification

The new system will assist to resolve the difficulty intrinsic in the current system by offering additional secured credit card operation using hybrid model for the fraud detection.

1. The hybrid technology of fraud discovery system is not having complex process in performing fraud check.

2. The new fraud discovery structure gives genuine and fast result than existing system.

3. The hybrid technology makes the processing of detection very simple and tries to remove the complexity.

4. Monitor more transactions in less time; with the new system, millions of transactions can he monitored in less time.
5. Conduct faster, more thorough investigations. it would enable card owners conduct a more thorough investigation on fraudulent activities since the system will automatically collect Internet Protocol (IP) address along with Geo-location of the intruder as well as his/her work station's

High Level Model of the New System

The high level Model of the new system shows that we have two dynamic players in the system the admin user and the customer user. Their activities on the system are divided as shown in figure 3.

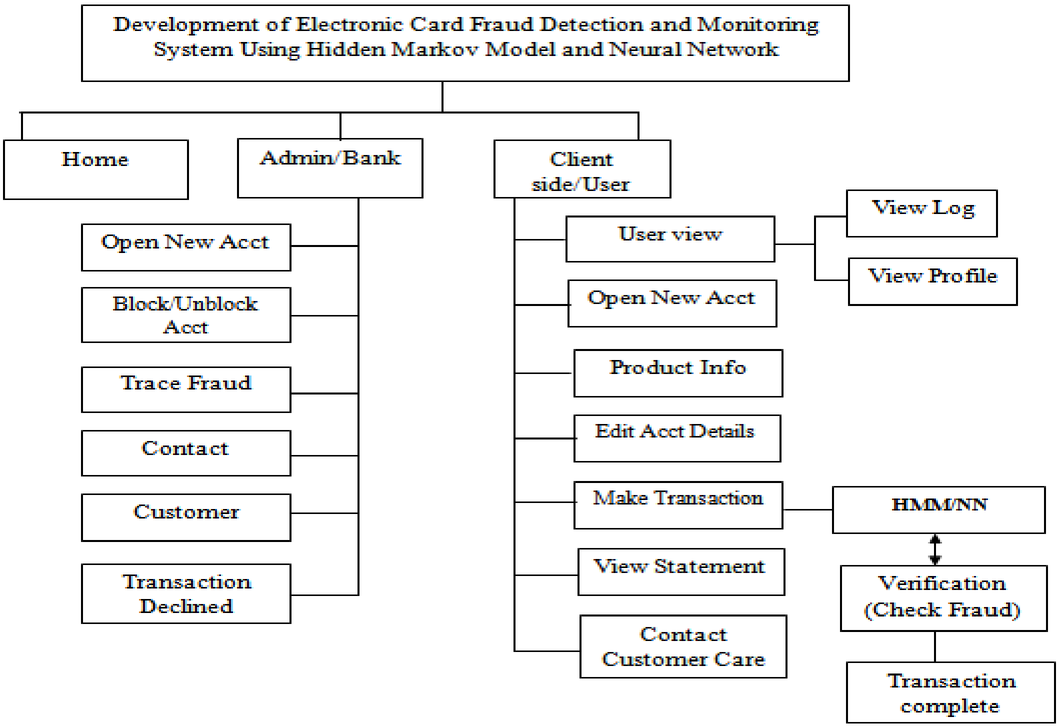


Figure 3: High level Model of the New System

Application of the design

1. Provide simple and refined security to virtual transactions
2. Present a proactive method of preventing or stopping human interference
3. To express a message notification to the core system, (client and bank) on any suspicious dealings during runtime

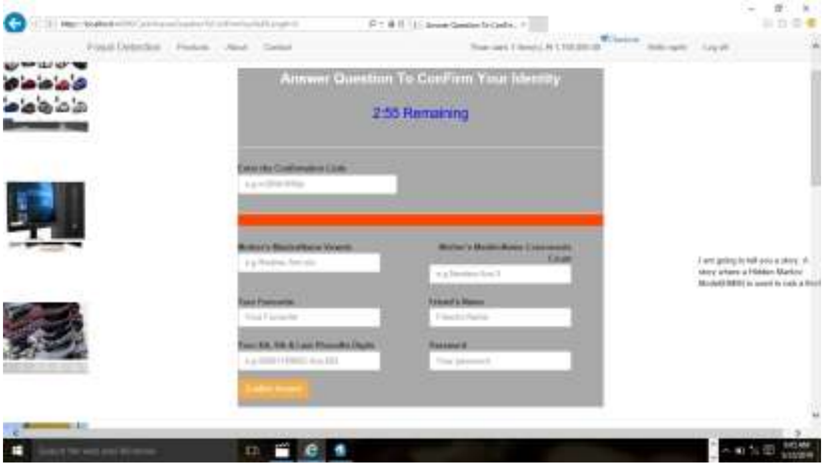
III. CONCLUSION

Efficient credit card fraud discovery system is extremely required for card issuing bank or all type of online transaction through using credit card. We have developed a hybrid technology approach in credit card fraud discovery. It easily detects and removes the complexity. It has as well elucidated how Hidden Markov Model and Neural Network can identify whether a transaction is fraudulent or not.

The end user is provided with a scalable security platform that is to be attached to the existing e-payment platform which will be employed to buy products and authenticate payments online.

The Hybrid technique is utilized to detect various unobserved (hidden) activities on credit cards. It maintains a database, where past records of transactions are saved. The owner is alerted through a system of messages if an abnormal operation has occurred that is unusual from the historical transaction records. The Credit Card Fraud Discovery System is also scalable for managing huge amount of transactions.

We suggested a system application of Hybrid model in abnormality or suspicious detection. The different steps in transaction of credit card management are embodied as the necessary technique of a hybrid method. The system application captures every the customers' detail and validates the data cautiously to identify virtual fraud; it has as well expressed how it can ascertain whether a current transaction is illegitimate or genuine. Additional security measures like security questions, confirmation code, shipping location details and IP address for verification detection are made available for an improved security and enhanced detection of illegitimate transaction. This recommended procedure can be advanced; and improved version can be developed



Answer Question To ConFirm Your Identity

2:55 Remaining

Password

Figure 4: customer secret questions and confirmation code form

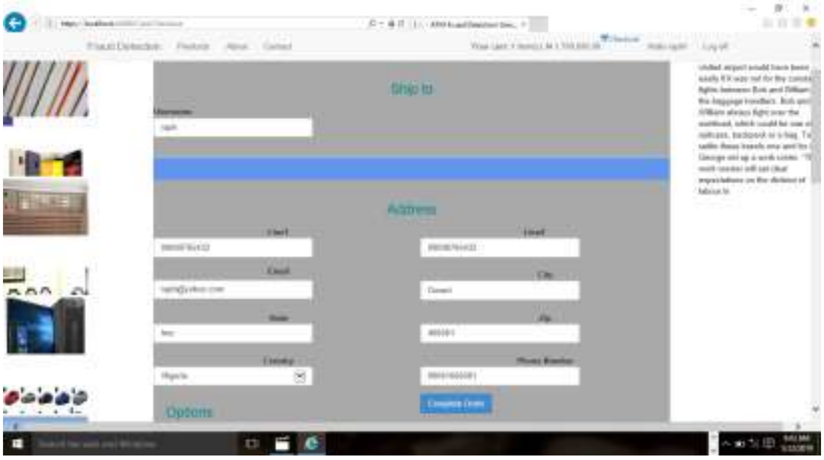


Figure 5: customer shipping loaction details form

REFERENCES

[1] Daigle and Lampe (2000). Electronic Business, Continuous Assurance, Fraud Detection, E-crime, eSCARF... as security, privacy and reliability concerns

[2] Elliot, S and Fowell. S (2000); Expectation versus reality; a snap shot of consumer experience with internet retailing, International journal of information management 323-336.

[3] Bhatla, T.P. Prabhu .V, Dua A, (2003): “Understanding Credits Cards Frauds” Card Business review. Tata Consulting Services. Available at http;//www.tes.com/0_whitepapers/htdocs/credit_card_fraud_white_paper_v_1.0.pdf

[4] Kim M.J. and Kim, T.S. (2002). A Neural Classifier with Fraud Density Map for Effective Credit Card Fraud Detection Proc. Int’l Conf. Intelligent Data Eng. and Automated Learning, pp. 378-383.

[5] Chiu A., Tsai C., (2004). A Web Services-Based Collaborative Scheme for Credit Card Fraud Detection. Proceedings of the IEEE International Conference on e-Technology, e-Commerce and e-Service, pp.:177-181

[6] Bolton, R. J. and Hand, D. J. (2001): “Unsupervised Profiling Methods for Fraud Detection,” in Proceedings of the Conference on Credit Scoring and Credit Control, Edinburgh, UK.

[7] Brause R., Langsdorf T., and Hepp M., (1999); Neural Data Mining for Credit Card Fraud Detection. Proc. IEEE Int’l Conf. Tools with Artificial Intelligence, pp.:103-106,