ANALYSIS AND DESIGN OF CREDIT CARD FRAUD DETECTION SYSTEM WITH OBJECT ORIENTED METHODOLOGY

AMANZE, B.C[1], CHILAKA, U.L[2], AGOHA, U.K[3]

ABSTRACT

Nowadays, the development of technology is rapidly increasing, including the credit card fraud. The credit card fraud (CCF) is one of the problem our banking system is facing today. Fraudsters used many methods to attack the customer. The growth in electronic transactions has resulted in a greater demand for fast and accurate user identification and authentication. Conventional method of identification based on possession of pin and password are not all together reliable. Higher acceptability and convenience of credit card for purchases have not only given personal comfort to customers but also attracted a large number of attackers. As a result, credit card payment systems must be supported by efficient fraud detection capability for minimizing unwanted activities by fraudsters. To deal with this problem, a computerized system is needed. Methods used in analyzing and designing of the credit card fraud is Object Oriented Analysis (OOA) with unified modeling language (UML).

KEYWORDS: : Credit Card, Object Oriented Methodology, Unified Modeling Language, Information System, Bank Staff and Bank Customer.

[1]Department of Computer Science, Faculty of Science, Imo State University, Owerri, Nigeria
[2,3] Ph.D Students, Dept. of Computer science, Faculty of Science, Imo State University, Owerri, Nigeria

HOW TO CITE THIS ARTICLE:
Dr. V Suresh (2019). An Approach of Checking Grammar for Telugu Language Complex Sentences, International Educational Journal of Science and Engineering (IEJSE), Vol: 2, Issue: 1, 18-25

INTRODUCTION

In credit or debit card based purchase, the cardholder presents card to a merchant for making payment. To commit fraud in this kind of acquisition, the fraudster has to steal the credit card. If the legitimate user does not understand the loss of card, it can lead to important financial loss to the credit card company and also to the user. In online payment mode, attackers need only little information for false transaction, for example, secure code, expiration date, card number and many other factors. In this purchase method, many transactions will be done through Internet or telephone. To obligate fraud in these types of purchases, an impostor simply needs to know the card details. Most of the time, the honest cardholder is not aware that someone else has seen or stolen his card information. The only way to detect this kind of fraud is to analyze the spending patterns on every card and to figure out any irregularity with respect to the "usual" spending patterns. The examination of existing purchase data of cardholder is a likely way to reduce the rate of positive credit card frauds. Since humans tend to display specific behaviorist profiles, every cardholder can be characterized by a set of patterns comprising information about the distinctive purchase category, the time since the last buying, the amount of money spent, and other things. Nonconformity from such patterns is reflected as fraud.

Credit card frauds are increasing day by day as the use of credit card is increasing [1]. Occurrence of credit card fraud has increased dramatically both online and offline. Credit card based purchase can be done in two ways: (i) physical card (ii) virtual card. In physical card purchase, the cardholder presents his card physically to the merchant for making payment. For this type of fraud the attacker has to steal the credit card. In virtual card purchase only the information about the card is stolen or gathered like card number, secure code etc. Such purchases are done over the Internet. For this type of fraud the attacker needs only the card details so the only way to detect this type of fraud is to analyze the spending pattern of the card holder. When one's credit card or credit card information is stolen and used to make unauthorized purchases on e-commerce systems on the Internet, one becomes a victim of internet credit card fraud or no card present fraud. This is nothing new and there is nothing unusual about this because identity theft and credit-card fraud are present-day happenings that affect many people and involve substantial monetary losses. Fraud is a million dollar business and increasing every year.

Credit card is refers to a method of selling goods or services without the buyer having cash in hand [2]. A credit card transaction involves four entities. The first entity is the consumer; that is the person who owns the card and who carries out the legitimate transactions. The second entity is the credit card issuer; that is usually the consumer's

Copyright© 2019, IEJSE. This open-access article is published under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License which permits Share (copy and redistribute the material in any medium or format) and Adapt (remix, transform, and build upon the material) under the Attribution-NonCommercial terms.

bank – also known as issuing bank – which provides the credit services to the consumer. The credit card issuer sends the bill to the consumer in order to request a payment for their credit card transactions. The third entity is the merchant who sells goods or services to the consumer by charging consumer's credit card. This charge is achieved through merchant's bank – the forth entity – which sends the request for the transaction to the issuing bank. The issuing bank will check whether the amount of the transaction does not reach the credit card's limit before authorizing that transaction. If the transaction is valid, the issuing bank will block the requested amount from consumer's credit card account and send an authorization response to merchant bank. As soon as the authorization response is received by the merchant's bank, the merchant is notified; the transaction is marked as completed and the consumer can take the goods. The blocked amount on consumer's credit card account will be transferred into merchant's bank account.

Statement of the Problem

Information Technology (IT) has contributed to a great extent in mitigating fraud for banks that have embraced and implemented it. Credit card transaction frauds cost financial institutions millions of dollars per year. As a result, fraud detection has become an important and urgent task for this business. The incidents of loss of hard earned money to fraudsters have raised a lot of concern and portend serious danger to economic growth. Ordinarily, thieves invade homes and offices to steal physical cash from their victims. The rapid development in information and communication technology has introduced a cashless society where people can pay for goods and services using credit cards. This appears more secured as people no longer keep huge physical cash at home; leading to less incidents of theft. The recent development shows that hackers have device electronic means of stealing money from people's account by stealing their credit card details and using same to transfer money to other accounts. This is heart breaking and requires an enhanced security system on communication channels to avert such financial loss. Another challenge for contemporary financial institutions is the ability to understand and deal with the high volume of data and information, and using knowledge from them to improve and make informed decisions. Credit card fraud detection is a pattern recognition problem. Every cardholder has a shopping behavior which establishes a profile for the cardholder. Currently, fraud detection system (FDS) identifies many legitimate accounts as fraudulent resulting in a large number of false positives (FPs). As every cardholder has a huge number of possibilities for developing new patterns of behavior, the types of transactions are widely variable. Hence, it is almost impossible to identify consistent and stable patterns for al1 the transactions. In fact, there are so many variations of behavior for each individual that are exponential in combination and the complexities of enumerating all combinations of cases are enormous. This ever changing pattern of behavior with the combination of legitimate and fraudulent cases has left the Financial Institutions (FIs) with a large number of FPs (approximately 90% of flagged accounts) for investigation. The above challenges can be addressed through the use of a multi-agents system that is based on artificial intelligence since it will provide managers with added value information reduce the uncertainty of the decision outcome and thereby enhance banking service quality. No doubt, the application of new technologies can give bank a competitive lead to a high performance and eliminate fraud associated with credit cards. Credit card frauds (CCF) have been a long –time headache for credit card companies. With the growth of online business in Nigeria, the number of credit card frauds has also increased drastically.

REVIEW OF RELATED LITERATURE

[3] Stated that today it is easy to do banking transaction digitally, both on a computer or by using a mobile phone. As the banking-services increase and get implemented to multi-platforms, it makes it easier for a fraudster to commit financial fraud. In their research, they discovered the need to focus on investigating log-files from a mobile money system that makes it possible to do banking transactions with a mobile phone. They developed a system whose main objective is to evaluate if it is possible to combine two statistical methods, Benford's law together with statistical quantiles, to find a statistical way to find fraudsters within a Mobile Money system. To achieve this, rules were extracted from a case study with focus on a Mobile Money system and limits were calculated by using quantiles. A fraud detector was implemented that uses these rules together with limits and Benford's law in order to detect fraud. The fraud detector used the methods both independently and combined.

Finally, the results obtained showed that it is possible to use the Benford's law and statistical quantiles within the studied Mobile Money system. It is also shown that there is only a very small difference when the two methods are combined or not both in detection rate and accuracy/ precision. Meanwhile, [3] concluded that by combining the chosen methods it is possible to get a medium-high true positive rates and very low false positive rates. The most effective method to find fraudsters is by only using quantiles.

[4] Proposed credit card fraud detection model using Hidden Markov Model. Hidden Markov Models (HMMs) which is a statistical tool and extremely powerful method used for modeling generative sequences characterized by a set of observable sequences. Hidden Markov Model is probably the simplest and easiest model which can be used to model sequential data, i.e. data samples which are dependent on each other. An HMM is a double embedded random process with two different levels, one is hidden and other is open to all. The Hidden Markov Model is a finite set of states, each of which is associated with a probability distribution. Transitions among the states are governed by a set of probabilities called transition probabilities. In a particular state, an outcome or observation can be generated according to the associated probability distribution. It is only the outcome, not the state visible to an external observer and therefore states are "hidden" to the outside; hence, the name Hidden Markov Model [5]. HMM has been successfully applied to many applications such as speech recognition, robotics, bio- informatics, data mining etc.

[4] Achieved their aim by storing all the information about credit card (Like Credit card number, credit card CVV number,

credit card Expiry month and year, name on credit card etc.) in the credit card database. If details entered by User into the database are correct then it will ask for Personal Identity number (PIN). After matching of Personal Identity number (PIN) with database and account balance of user's credit card is more than the purchase amount, the fraud checking module will be activated. The verification of all data will be checked before the first page load of credit card fraud detection system. If user credit card has less than 10 transactions then it will directly ask to provide personal information to do the transaction. Once database of 10 transactions is developed, then fraud detection system will start to work. Observation probabilistic in an HMM Based system is initially studied, spending profile of the cardholder and followed by checking an incoming transaction against spending behavior of the cardholder one can show clustering model is used to classify the legal and fraudulent transaction using data conglomeration of regions of parameter, HMM based credit card fraud detection during credit card transaction. [4] Presented experimental result to show the effectiveness of our approach.

METHODOLOGY ADOPTED

Object-oriented analysis and design methodology (OOADM) which is adopted in this dissertation is a set of standards for analysis and development of the credit card fraud detection system. It uses a formal methodical approach to the analysis and design of information system. Object-oriented design (OOD) elaborates the analysis models to produce implementation specifications. The main difference between object-oriented analysis and other forms of analysis is that by the object-oriented approach one organize requirements around objects, which integrate both behaviors (processes) and states (data) modeled after real world objects that the system interacts with. In other traditional analysis methodologies, the two aspects: processes and data are considered separately. For example, data may be modeled by ER diagrams, and behaviors by flow charts or structure charts. The primary tasks in object-oriented analysis (OOA) are:

a.Find the objects and organize them
b.Describe how the objects interact
c.Define the behavior of the objects
d.Define the internals of the objects

Common models used in OOA are use cases and object models. Use cases describe scenarios for standard domain functions that the system must accomplish. Object models describe the names, class relations (e.g. Circle is a subclass of Shape), operations, and properties of the main objects.

Analysis of the Credit Card

However, the protocol for performing credit card transactions is composed of two query-response pairs. First, the Point-of-Sale solicits credit card number and expiration date, and the card responds with this information. In its response, the credit card also includes an iCVV, or integrated Card Verification Value: a dynamic security token intended to authenticate the message. Once this has been completed, the Point-of-Sale sends a charge request to the bank with the information received from the credit card, and then receives an authorization response to accept or reject the charge. Fig. 1.1 shows the current credit card (CC) protocol.

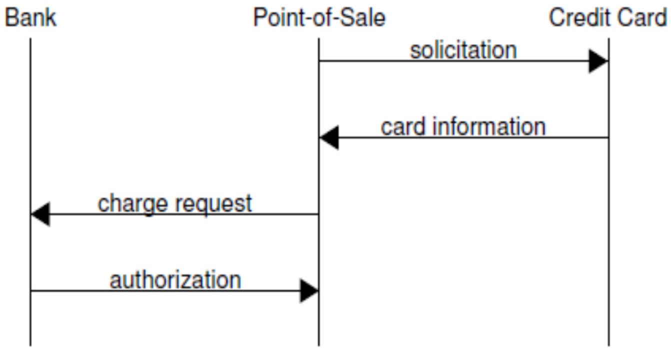


Figure 1: The CDurrent Credit Card Protocol

The exchange of messages in the CC Protocol is shown in Fig. 1. They are: solicitation, card information, charge request and authorization. Note that after the card responds to the Point-of-Sale, its involvement in the transaction is complete. The contents of these messages are as follows:

Solicitation: First, the Point-of-Sale solicits the credit card for its information. The solicitation is composed of a number of messages sent in both directions, identifying the Point-of-Sale type (e.g. 2PAY.SYS.DDF01) and the credit card type (e.g. VISA CREDIT). Since these messages are constant for a given Point-of-Sale and credit card, we abstract the solicitation messages as a single request from the Point-of-Sale to the credit card.

Card Information: The credit card responds to the solicitation by sending back the following card information:

1. The credit card number
2. The credit card's expiration date
3. The iCVV
4. The name of the bank that issued the card

The iCVV is an unpredictable 4-byte value freshly generated for every solicitation response, and is subsequently used by the bank to validate the transaction as described below.

Charge Request: The Point-of-Sale issues a charge request to the bank. This request is composed of:

1. The credit card number
2. The credit card's expiration date
3. The iCVV
4. The amount to be charged

Authorization: When the bank receives a charge request, it uses the credit card number to look up the account, verifies the expiration date, and then validates the iCVV to authorize the purchase. It will generally also perform some additional checks, such as verifying that the card was not reported lost or stolen, or matching this purchase's location against the known location of the card holder. Finally, it responds with its authorization decision.

When the credit card is manufactured, a secret seed value is shared between the credit card and the bank. This enables the credit card and the bank to both generate the same iCVV sequence, unpredictable to any party that does not have access to this seed. The iCVVs are simply sequential elements of this sequence: each time the credit card responds to a solicitation, it generates the next iCVV in the sequence and includes it with the card information response. In order to make an authorization decision, the bank searches through its account database which is indexed by the credit card number. Once the bank locates the account, it verifies that the received expiration date matches the expiration date on file. In addition, it recalls the iCVV from this credit card's previous charge request and generates the next element in the sequence, then compares the received iCVV to the value it generated.

It is possible that a card may generate an iCVV without communicating it to the bank. For example, a charge request may become corrupted in transit, or a Point-of-Sale may experience a network failure. As a result, a credit card's iCVV may have advanced further in the sequence than the bank expects. To handle this situation, the bank may generate several iCVVs in the sequence for comparison to the received value. If a match is found, the bank considers the iCVV to be valid. It updates its state into the pseudorandom sequence to reflect the received iCVV, and continues with any other checks to be performed before authorizing the charge. If no match is found, the bank considers the iCVV to be invalid and declines the charge.

Use Case Diagram of the Credit Card Fraud

The model designed in this paper is divided into several modules that needs access restrictions. Different use cases were described in the way they were applicable in the software designed. Use cases are as listed below:

1. Bank staff Use Case
2. Credit card holder Use Case
3. Use Case diagram of the New System.

Use Case Boundary of Bank Staff

The system identified total of two roles that functions as access levels in the diagrams. A use case is a function to be performed by the system from the user's perspective. Fig. 2 is the use case boundary diagram of the new system. Fig. 2 represents the bank staff use case diagram. The bank staff will have access to opening a new account to customers, issue credit card pin to customers, credit or debit customers account during normal banking transaction within the banking hall.

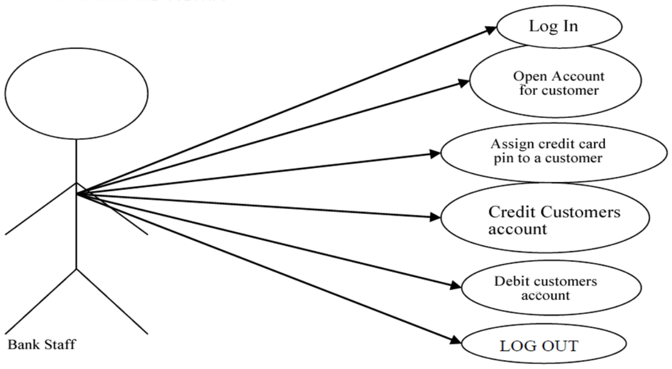


Figure. 2: Use Case Boundary of Bank Staff

Use Case Boundary of Credit Card Holder

The credit card holder can login to the system using credit card pin and username. The user can perform credit card transactions, view account balance, view account statement and also have access to changing the credit card pin as shown in Fig. 3.

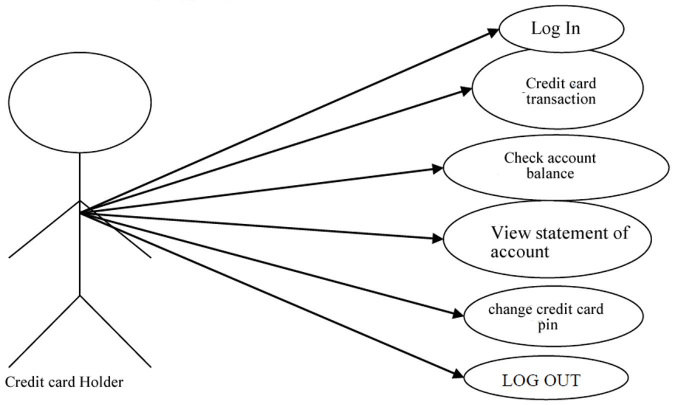


Figure 3: Use Case Boundary of Credit Card Holder

Use Case Diagram of the New System

Fig 4. Shows a use diagram of the new system, the large rectangle is the system boundary. Everything inside the rectangle is part of the system under development. Outside the rectangle are the actors that act upon the system. Actors are entities outside the system that provide the stimuli for the system. Typically, they are human users, or other systems. Inside the boundary rectangle are the use cases. These are the ovals with names inside. The lines connect the actors to the use cases that they stimulate.

a. An <<includes>> relationship indicates that the second use case is always invoked by the first use case.
b. An <<extends>> relationship indicates that the second use case may optionally invoke the first use case.

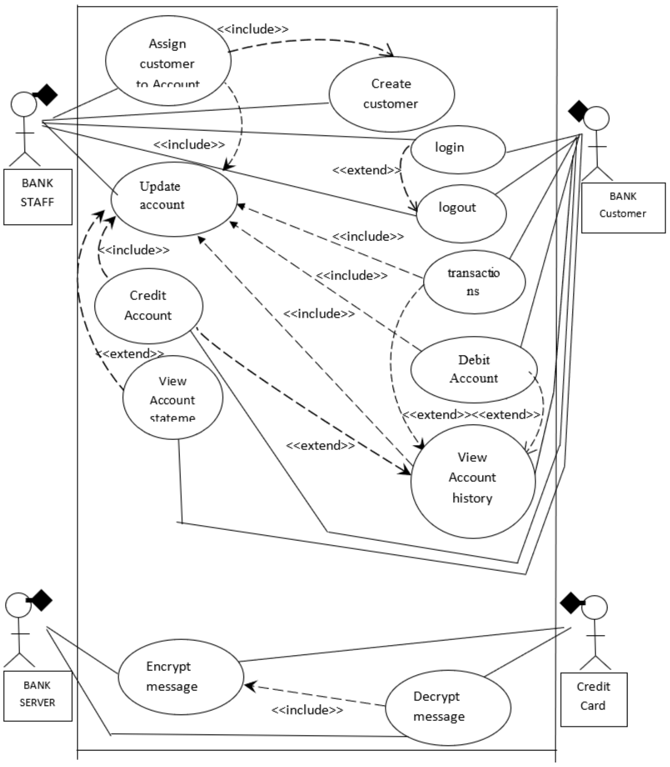


Figure 4: Use Case Diagram of the Credit card

Object Diagrams

Sequence Diagram of the Credit Card Transactions

Figure 5. Contains the following below:

New Credit card: Given Input- Request from the user for the card. Expected Output-Assigning an account to requested user.

Login: Given Input- Give username and password of particular user.
Expected Output- Login to user's account.

Security information: Given Input- Give the security information by answering security questions. Expected Output-Update of account with the security details.

Transaction: Given Input- Give the credit card details and performs transaction.
Expected Output- Update database.

Verification: Given Input- Checks with user's stored details like security answers or previous spending profile.
Expected Output-If the verification is success, user can perform transaction, else blocks the card.

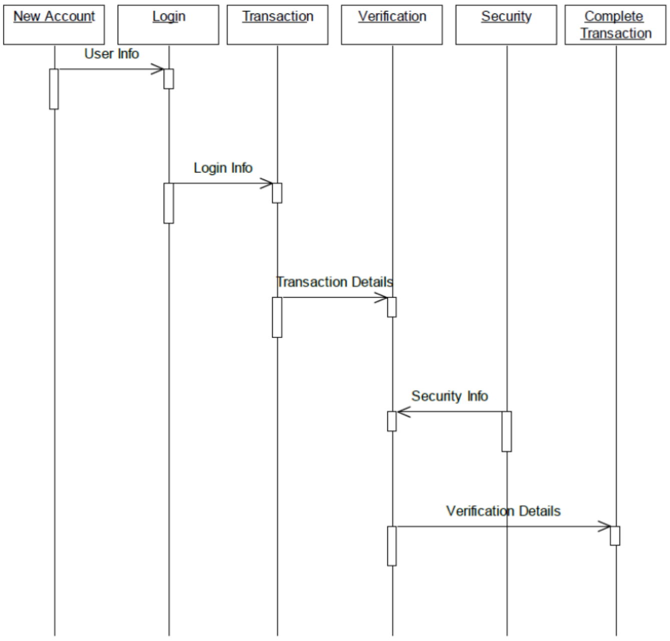


Figure 5: Sequence Diagram of Credit Card Transactions

Sequence Diagram of the Credit Card Transaction

Fraud Management Filters checks for payment characteristics that may indicate fraudulent activity. Fig. 6 set up Fraud detection Filters to provide the tightest control possible over payments so that you can deny payments that are likely to result in fraudulent transactions and accept payments that are not typically a problem. The customer initiates the online payment transactions, the multi-agents verifies the customers previous spending profile through the use of data mining and confirms the payment where the profile not suspicious otherwise the transaction is blocked. The bank processes the payment.

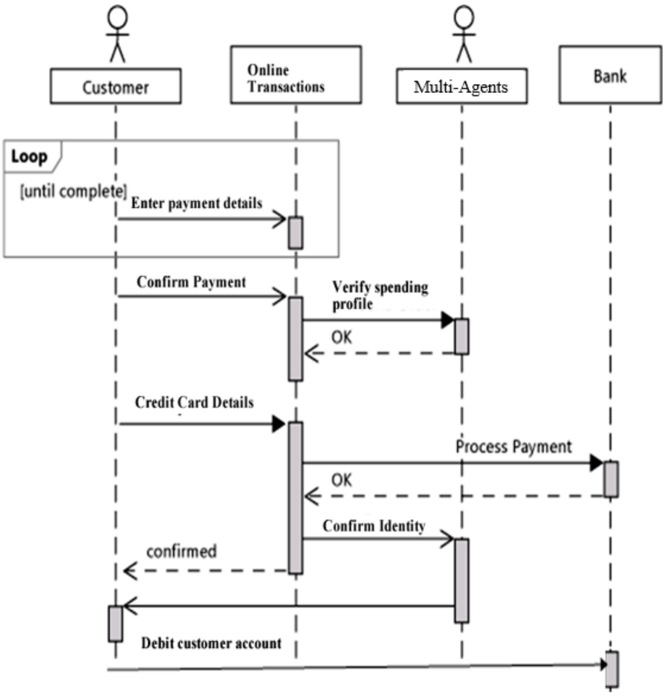


Figure 6: Sequence Diagram of the New System

State Diagram of Credit Card Transactions

Fig. 7 shows the four states of the transactions. First the credit card user makes request for to use the credit card platform, provide credit card information and login. Then finally complete the transaction.

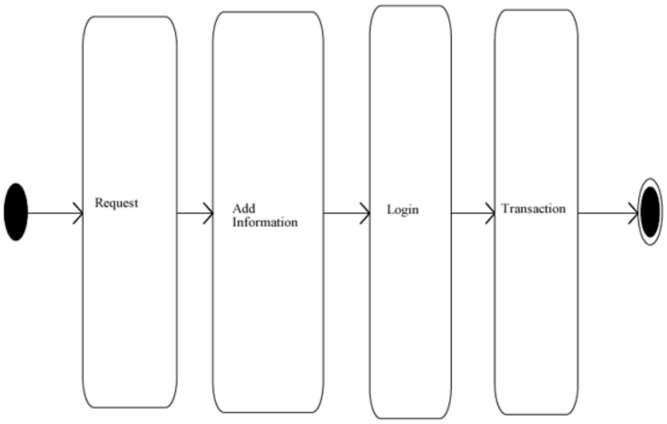


Figure 7: State Diagram of Credit Card Transactions

Activity Diagram of the Credit Card Fraud Detection System
Fig. 8 shows the various processes that lead to credit card transactions. It starts with opening a credit card account, making purchase online, effecting payment with your credit card which will be verified before the transaction is completed.

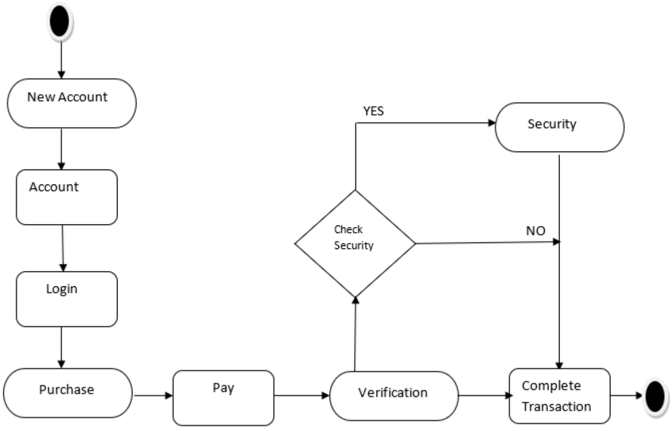


Figure 8: Activity Diagram of Credit Card Transactions

Collaboration Diagram of Credit Card Transaction

Fig. 9 shows the various information that needed at each stage of the credit card transactions.

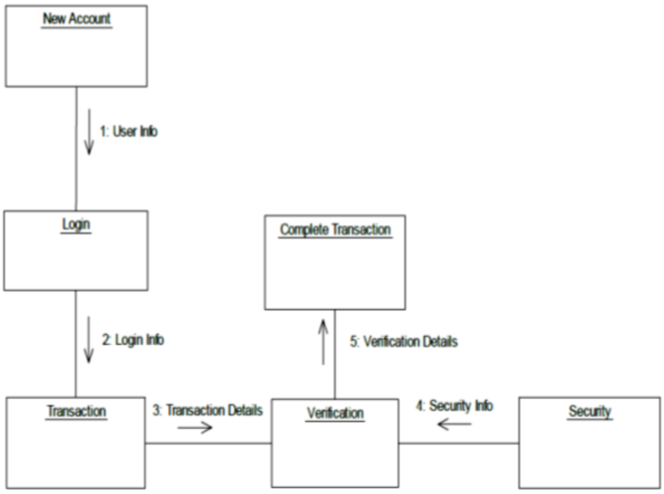


Figure 9: Collaboration Diagram of Credit Card Transactions

Event Package Diagram

The event package diagram as shown in Fig. 10 shows the various stages of events in the process of using credit card for payment. It starts with entering the card details which needs to be verified before completing the transaction.

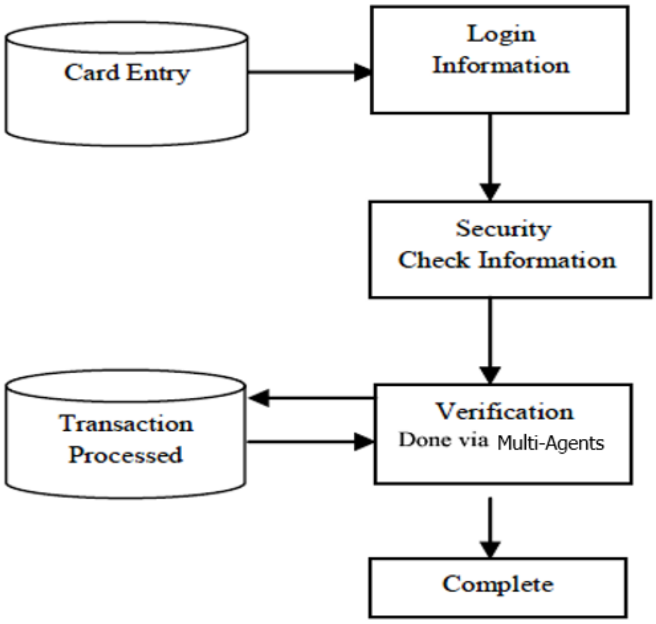

Card Entry
Login Information
Security Check Information
Verification Done via Multi-Agents
Transaction Processed
Complete

Figure 10: Event Package Diagram of Credit Card Transactions

Class Diagram of the New System

Fig. 11 show the database class diagram of the new system. The line shows the associations between the various tables in the database.

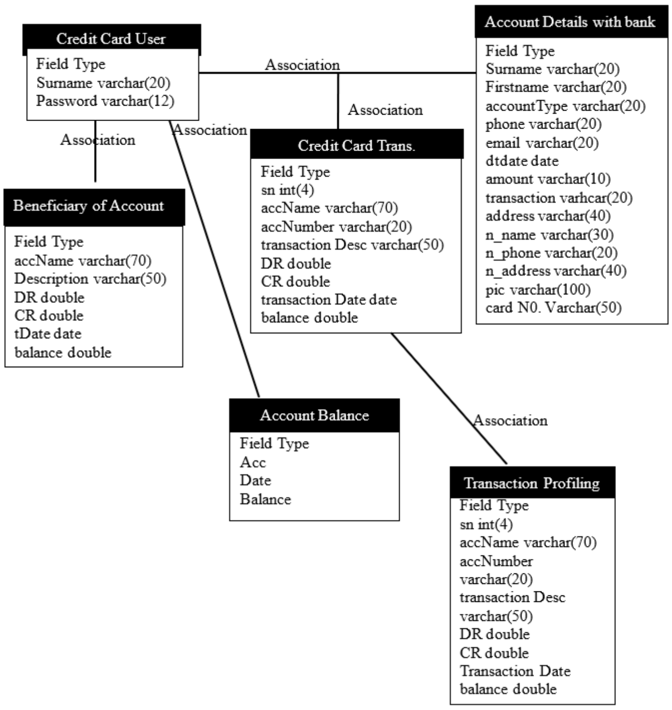


Figure 11: Class Diagram of the Credit Card Fraud Detection System

Entity Relationship Diagram of the New System: Entity Relationship diagrams is a specialized graphics that illustrate the interrelationship between entities in a database. Fig 12 shows the entity relationship in the database. The diagram above is an entity relationship diagram that is a major data modeling tool that helped database analysts to organize data into entities.

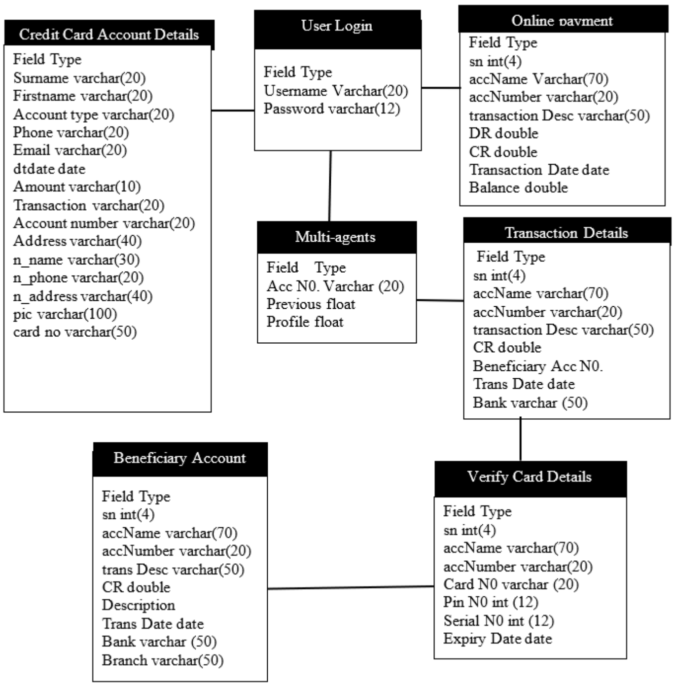


Figure 12: Entity Relationship Diagrams of Credit Card Transactions

a. The Structure of the Display

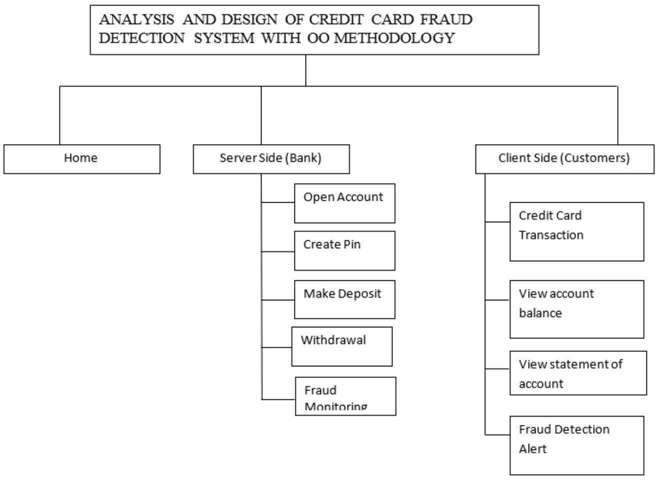
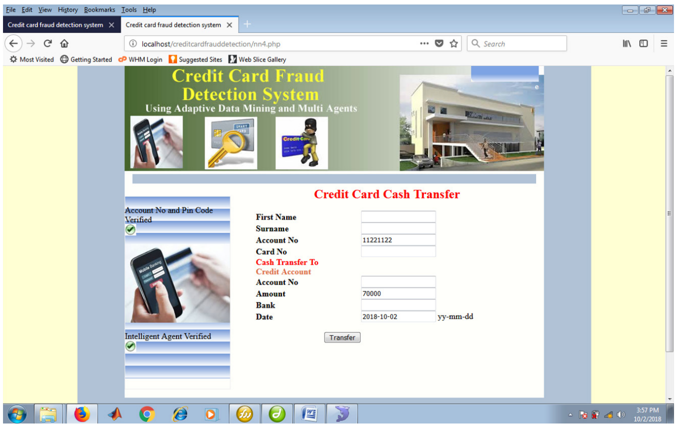


Figure13: Display Structure

b. Draft Screen


File Edit View History Bookmarks Tools Help
Credit card fraud detection system
localhost/creditcardfrauddetection/nn4.php
Search
Most Visited
Getting Started
WHM Login
Suggested Sites
Web Slice Gallery
Credit Card Fraud
Detection System
Using Adaptive Data Mining and Multi Agents
3:57 PM
10/2/2018

Credit Card Cash Transfer

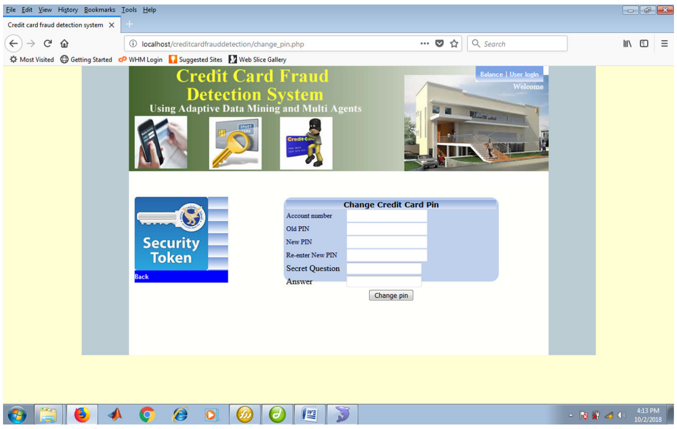
Account No and Pin Code Verified ✓

Intelligent Agent Verified ✓

First Name	
Surname	
Account No	11221122
Card No	
Cash Transfer To Credit Account	
Account No	
Amount	70000
Bank	
Date	2018-10-02 yy-mm-dd

Transfer

Figure 14. Credit Card Details Verification Form


File Edit View History Bookmarks Tools Help
Credit card fraud detection system
localhost/creditcardfrauddetection/change_pin.php
Search
Most Visited
Getting Started
WHM Login
Suggested Sites
Web Slice Gallery
Credit Card Fraud
Detection System
Using Adaptive Data Mining and Multi Agents
Balance | User login
Welcome
Security Token
Back
4:13 PM
10/2/2018

Change Credit Card Pin

Account number	
Old PIN	
New PIN	
Re-enter New PIN	
Secret Question	
Answer	

Change pin

Figure15: Customer Account Pin Change Form

CONCLUSION

The work developed a new object oriented approach of solving bank frauds problems especially in the area of credit card fraud. A conceptual framework for a system based on credit card fraud (CCF) process was developed. Various classes of object diagrams were proposed to provide a set of functionalities for CCF in electronic environment for banks.

REFERENCES

1. Patel, Twinkle, & Ompriya, Kale. (2014). A Secured Approach to Credit Card Fraud Detection using Hidden Markov Model. International Journal of Advanced Research in computer Engineering and technology, 3(5), 1576.
2. Delawaire, L., Hussein, A.,& John P (2009). Credit Card Fraud and Detection Techniques: A Review, International of Journal of Technology and, 4(2), 57-68.
3. Kappelin, F. and Rudvall, J. (2015): "Fraud Detection within Mobile Money: A mathematical statistics approach" MSc Thesis submitted to the Dept. Computer Science &Engineering Blekinge Institute of Technology SE–371 79 Karlskrona, Sweden.
4. Khan, A. P., Mahajan, V. S., Shaikh, S. H and Koli, A. B. (2013): "Credit Card Fraud Detection System through Observation Probability Using Hidden Markov Model" International Journal of Thesis Projects and Dissertations (IJTPD) Vol. 1, Issue 1, PP: (7-16), Month: October-December 2013, Available At: www.researchpublish.com
5. Ghosh and Reilly (2014). Credit Card Fraud Detection with a Neural Network. IEEE Proceedings of the Twenty-Seventh Annual Hawaii International Conference on System Sciences, 3, 621-630.
6. Patidar, R., &Sharma, L. (2011). Credit Card Fraud Detection using Neural Network. International Journal of Soft Computing and Engineering, 1(2), 2231-2307.
7. Osama, D., Phudung, L., & Bala, S. (2008). Fraudulent Internet Banking Payments Prevention using Dynamic Key. Journal of Networks, 3(1).