Adaptive Data Mining and Intelligent Agent Framework for Credit Card Fraud Detection

Nwabrije, L.E & Anireh, V.I.E
Department of Computer Science
River State University of Science & Technology
Port-Harcourt, River State, Nigeria.
E-mails: nwabrije.loveth@gmail.com, anireh.ike@ust.edu.ng

ABSTRACT

In this study, credit card fraud detection was investigated using Artificial Intelligent machine learning and data mining technique. Input data to the system was empirical dataset whose patterns contain fraudulent behaviors. Experiment performed includes mining these patterns and classifying them into optional clusters. The system was designed using Java programming language at the front end and MySQL at the backend. A new dataset was used to test the system and result obtained showed improved accuracy that compares with that quoted in the literature. The system can be deployed in online payment platforms and financial institutions where credit card businesses are mostly transacted.

Keywords: Artificial Intelligent, Machine learning, Credit card fraud, Data mining

CISDI Journal Reference Format
Nwabrije L.E & Anireh V.I.E (2019): Adaptive Data Mining and Intelligent Agent Framework for Credit Card Fraud Detection. Computing, Information Systems, Development Informatics & Allied Research Journal. Vol 10 No 3, Pp 103-116. Available online at www.cisdijournal.org.
DOI Affix - https://doi.org/ 10.22624/AIMS/CISDI/V10N3P9

1. INTRODUCTION

Credit cards is an instrument in our every day life for purchasing goods and services by way of online transaction or physical card for offline transaction. In credit or debit card based purchase, the cardholder presents his card to a merchant for making payment. The occurrence fraud in this kind of acquisitions, the person 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 doing false transaction example secure code, expiration date, card number and many other factors. In this purchase method, mainly 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 (Adepoju, and Alhassan, 2010). Nonconformity from such patterns is reflected as fraud.

Credit card frauds can be broadly classified into three categories, that is, traditional card related frauds (application, stolen, account takeover, fake and counterfeit), merchant related frauds (merchant collusion and triangulation) and Internet frauds (site cloning, credit card generators and false merchant sites).

Data mining also known as knowledge discovery refers to a family of machine learning techniques capable of analyzing and extracting non-trivial patterns from data (Chen *et al*., 2004). Given that databases are too large; it is very inconvenient and impractical to look manually for hidden patterns on the data. Using Data mining technique, a lot previously hidden information in a data pattern can be made available for organizational decision-making process. Hormozi *et al*., (2004) described the advantages of such information discovery to an organization, which includes focusing on the most important information in a database to improve marketing strategies, and predicting future trends and behaviors.In this presentation, Data mining was applied to detect fraudulent credit card transactions, predict which customers are more likely to default their contractual obligations as well as identify fraudulent credit applications. Srivastava *et al*., (2008) stated that the only way to detect credit card fraud is by analyzing the spending behavior of customers. Kundu *et al*., (2004) added that customers tend to follow a standard spending profile and therefore any transaction that deviates from that standard can be considered suspicious. Such suspicious transactions can further be investigated in detail to determine whether they are indeed fraudulent or not. Using Data mining to analyze patterns and trends, financial Institutions can predict, with increased accuracy, how customers will react to adjustments in interest rates, which customers will be at a higher risk for defaulting on a loan, and how to make customers relationships more profitable. Historical default patterns can also help in predicting future defaults when same patterns are discovered (Costa *et al*., 2007). Data mining techniques are applied to enhance the accuracy of credit scores and predict default probabilities (Li and Liao, 2011). Credit score can be derived using the past behaviors of the borrower related to debt repayments by analyzing available credit history (He *et al*., 2010). Credit score is a value representing a borrower's creditworthiness. Behavioral scores are obtained from probability models of customer behavior to forecast their future behaviors in various situations.

2. REVIEW OF RELATED WORKS:

Credit card fraud detection has been an active research area. In Aleskerov (2007), a database mining system CARDWATCH, was developed for credit card fraud detection. The system, based on a neural learning module, provides an interface to a variety of commercial databases. Brause et al. (2008) developed an approach that involves advanced data mining techniques and neural network algorithms to obtain high fraud coverage.

Stolfo et al. (2010) proposed a credit card fraud detection system (FDS) using meta-learning techniques to learn models of fraudulent credit card transactions. Meta-learning is a general strategy that provides a means for combining and integrating a number of separately built classifiers or models. A meta-classifier was trained on the correlation of the predictions of the base classifiers. The same group also worked on a cost-based model for fraud and intrusion detection. They used Java agents for Meta-learning (JAM), which is a distributed data mining system for credit card fraud detection. A number of important performance metrics like True Positive-False Positive (TP-FP) spread and accuracy were also prescribed and their work was based on artificial intelligence combined with inductive learning algorithms and meta-learning methods for achieving higher accuracy.

Phua et al. (2014) suggested the use of meta-classifier similar to in fraud detection problems. They considered naïve Bayesian, and Back Propagation neural networks as the base classifiers. A meta-classifier was used to determine which classifier should be considered based on skewness of data. Although they do not directly use credit card fraud detection as the target application, their approach is quite generic.

Priyanka et al., (2016) presented system using HMM to detect the credit card fraud transactions by maintaining the database of spending behaviors of cardholders. The detail of items purchased by individual transactions is usually known to any fraud detection system running at the bank that issues credit cards to the cardholders. The system has security levels i.e. the security questions and the OTP.

3. MATERIAL AND METHODS

3.1 Materials

Fraud detection techniques now involves sophisticated screening of transactions to tracking customer behavior and spending patterns. They are being developed and employed by both merchants as well as card issuer banks. Some of the recently employed techniques include:

1. Transaction screening through Address Verification Systems (AVS)
2. Card Verification Method (CVM)
3. Personal Identification Number (PIN) and Biometrics.

AVS involves verification of address with zip code of the customer while CVM and PIN involve checking of numeric code that is keyed in by the customer. Biometrics might involve signature or fingerprint verification. Rule-based methods and maintaining of positive and negative lists of customers and geographical regions are also used in practice. Data mining and credit scoring methods focus on statistical analyses and deciphering of customer behavior and spending patterns to detect frauds (Huang, 2007). Neural networks are capable of deriving patterns out of databases containing historical transactions of customers. These neural networks can be ‘trained’ and are ‘adaptive’ to the emerging new forms of frauds. Deployment of sophisticated techniques and screening of every transaction alone will not reduce losses. It is necessary to employ an effective and economical solution to combat fraud. Such a solution should not only detect fraud cases efficiently but also turn out to be cost-effective. The idea is to strike a balance between the cost involved in transaction screening and review and the losses due to fraudulent cases. Analyses show that review of only 2.0% of transactions can result in reducing fraud losses accounting to 1.0% of total value of transactions. While a review of as high as 30% of transactions can reduce the fraud loses drastically to 0.06%, but that increases review costs exorbitantly.

The key to minimize total costs is to categorize transactions and review only the potentially fraudulent cases. This should involve deployment of a step-by-step screening, filtering and review mechanism. A typical deployment can involve initial authentication of transactions through PIN, expiry date on card, AVS and CVM. A second level of screening can involve comparing with positive and negative lists as well as rules based on customers geographical regions, IP addresses and policies. Risk and credit scoring with pattern and behavior analyses can come next, followed by manual review. This classifies and filters out transactions as genuine or fraudulent in every step and as a result only a few transactions would require further manual review. Such a solution reduces the overall processing delay as well as total costs involved in manpower and administration.

The existing systems adopted pin or biometric or data encryption or HMM, and other fraud detection technique. Most of these techniques have their setbacks. Attempt to use two level authentications yielded a better security system but still has some security challenges. Since the use of one factor or two factor authentication is still prone to security treats, this forms the major research gap. So the researcher proposes adaptive data mining and intelligent agent’s authentication system in our model.

3. 2 Methods

Object-oriented analysis and design methodology (OOADM) was adopted in this study because of its formal methodical approach to the analysis and design of information system. It elaborates the analysis models to produce implementation specifications and organizes requirements around objects, integrates both behaviors (processes) and states (data) modeled after real world objects that interacts with the system.

3.3 Analysis of the Existing System

In the existing system, the credit card holder supplies his/her username, password or Personal Identity Number (PIN), then the system validates the user identity by requesting for user account information from the customer's database. At that point, decision is taken as regards the customer's information. If the verification of the customer's information is valid, the transaction will be completed and account updated, but if invalid, access will be denied. The same process takes place with customers making payment for purchases using credit card. This process reduces stress of carrying so cash around, queuing up in the banking hall to make withdrawals, which reduces the workload on bank workers.

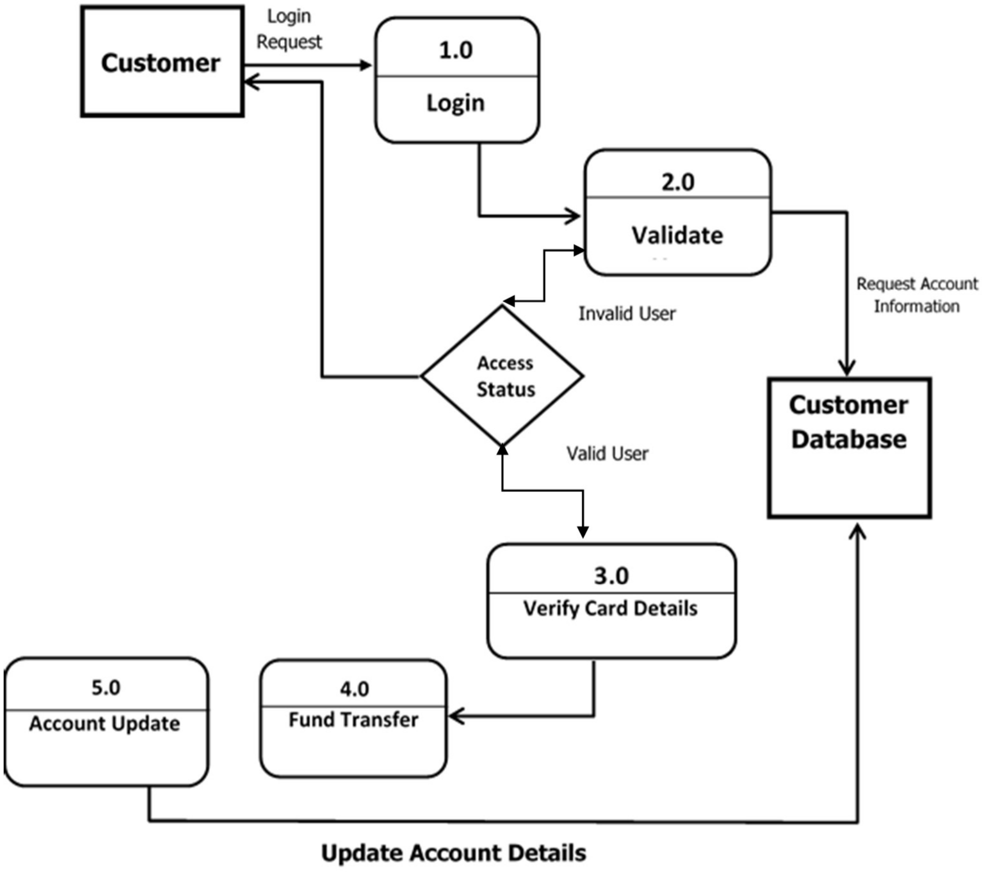


Fig. 3.1 Dataflow diagram of the existing system of credit card transaction

3.4. Analysis of the New System

Even though no system can be said to be 100% intrusion free, some measure of tuning can help prevent fraud in the credit card transaction and that is what is presented in this section. The proposed design system has three data mining engines: customer/bank database, credit card transaction database and fraud detection database. The customer/bank database has the following: opening of account operation, withdrawal and deposit transaction and credit card transaction. Fraud techniques database will give details of attack attempts on customer's credit card. The credit card database will contain all the previous credit card transactions carried out by the customer. The proposed system will detect the credit card fraud by analyzing the spending patterns on every card and flag any inconsistency with respect to the usual spending patterns. The Intelligent agent will make use of these inputs (from user transaction input and past recorded credit fraud detection input) watch ongoing transaction to check whether it is fraudulent or not, beginning from the most recent attack methods of fraudsters and concentrating the most recent spending pattern of the transaction.

3.5 System Operation

When a credit card transaction is initiated, the system verifies the user's pin code and username by validating it on the Database. If the pin fails to validate after three consecutive attempts, the account will be blocked and fraud alert flag sent to the fraud database. However, 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 will use the last ten credit card transaction to build a transaction pattern for the customer and forward the pattern to the collecting agent. The data collection agent will also use data mining technique to retrieve previous credit card fraud patterns from the credit card database and also retrieve the customer details from the database. The collection agent uses three sub-agents: query, mining, and result. However, the collection agent is 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 will match 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 sent to the reporting agent. The reporting agent will then forward the extracted credit card transaction status to the database and the customer's phone and the transaction blocked. However, if where the credit card profile matched with the existing customer profile, the transaction is allowed to go through and the customer's account updated accordingly either debited or credited. The system operation above can be depicted in processes shown in architecture of the proposed system in fig. 3.2.

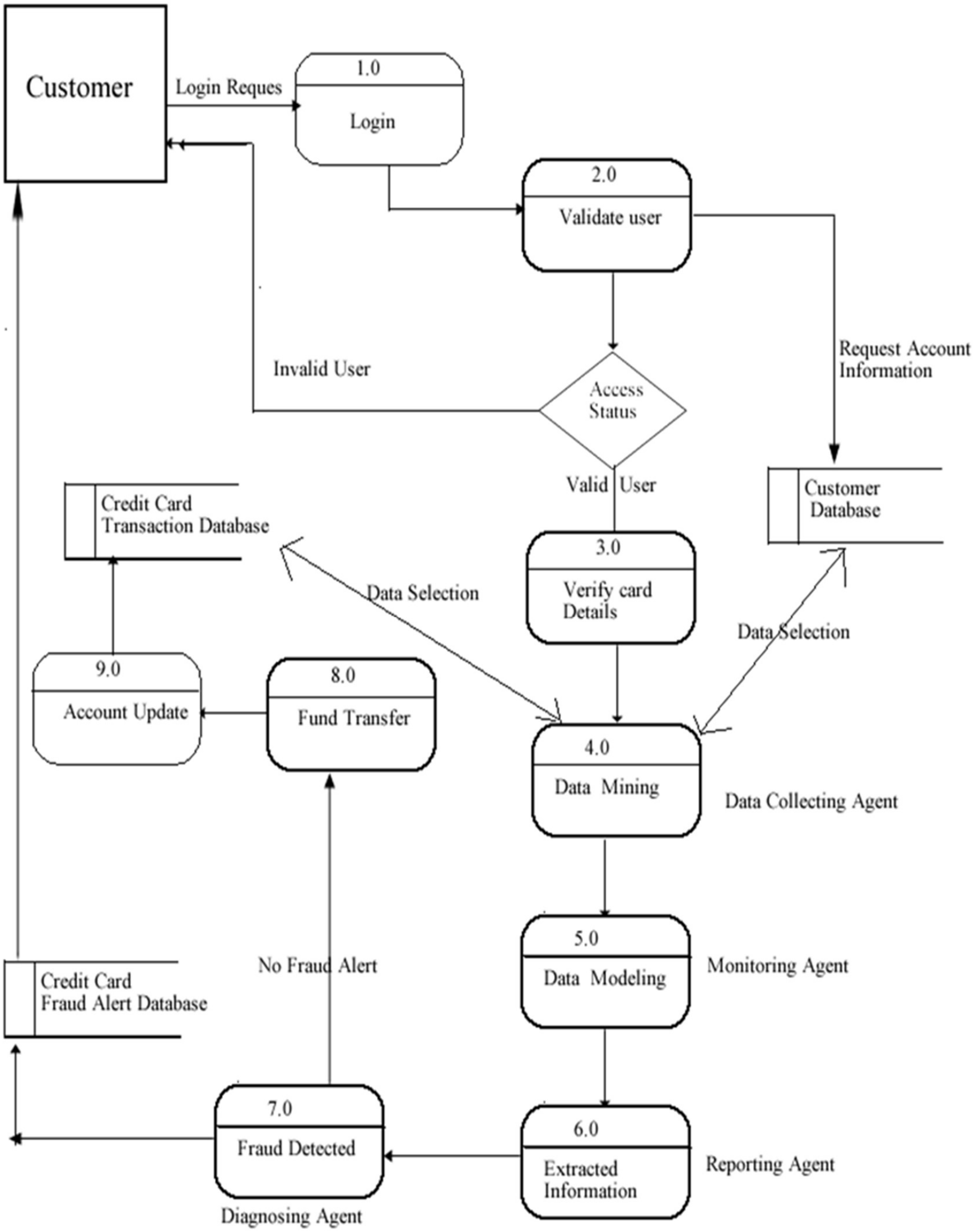


Fig. 3.2 Architecture of the proposed system

ALGORITHM

Given :

Accts: set of all accounts

Rules: set of all fraud rules generated from Accts

Input Phase: user inputs the credit card transaction details

User posts into core system and transaction is stored into the daily transactions table

Transaction Agent captures the Account Number being posted

Transaction Agent passes the number to intelligent agents

Intelligent agents check on rule set against the Account number received

Training Phase: Cluster creation

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

```
/*Initialization*/
S = { };
for (a ∈ Accts) do Cover[a] = 0;
for (r ∈ Rules) do
    Occur[r] = 0; /*Number of accounts in which r occurs*/
    AcctsGen[r] = { }; /*Set of accounts generating r */
end for
Check the previous spending profile
for (a ∈ Accts) do
    Ra = set of rules generated from a;
    for (r ∈ Ra) do
        Occur[r] : = Occur[r] + 1;
        add a to AcctsGen[r];
end for; end for
if transaction is outside spending profile alert is sent to monitoring agent
for (a ∈ Accts) do
    Ra = secret questions;
    request for user to supply secret question and answer
    while (cover[a] < Trules) do
        r := correct from Ra
        Remove r from Ra
        if (r ∉ S and Occur[r] ≥ Taccts ) then
            add r to S;
            for (a2 ∈ AcctsGen[r]) do
                Cover[a2] = Cover[a2] + 1;
            end for; end if
    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.

4. EXPERIMENT AND RESULTS

4.1 Experiments

The procedure above including other routines were coded in PHP, Java and MySQL database respectively. The front-end serves as input or data receptor while the backend accumulates stores and provides the acquired information as the need arises. The hardware requirement includes at least a 2.4 GHZ Intel Pentium Dual Core processor speed, 2GB RAM, 80 GB of Hard disk running Windows XP, Windows 2000, Windows 7 or Windows 8 with a fast Internet facility.

Table 4.1: Number of Passes and failures from users

S/N	SURNAME	FIRST NAME	ACCOUNT TYPE	ACCOUNT NUMBER	CC FRAUD PASSESD	CC FRAUD FAILED
01	OKWARA	NOBERT	CURRENT	0012345601	PASSED	
02	AHIAKWO	FAITH	CURRENT	0012345602	PASSED	
03	SYLVANUS	OGECHI	CURRENT	0012345603	PASSED	
04	OKORO	DANIEL	SAVINGS	0012345604		FAILED
05	AMADI	HENRY	SAVINGS	0012345605	PASSED	
06	IKEH	KATE	CURRENT	0012345606	PASSED	
07	ONAH	JAMES	SAVINGS	0012345607		FAILED
08	AMANZE	JOHN	SAVINGS	0012345608	PASSED	
09	NWOSU	IKECHUKWU	SAVINGS	0012345609	PASSED	
10	NWAOBILOR	ADAOBI	CURRENT	0012345610	PASSED	
11	BRIGGS	WHITE	SAVINGS	0012345611		FAILED
12	WIFA	BARIDO	SAVINGS	0012345612	PASSED	
13	AMADI	OLUCHI	CURRENT	0012345613	PASSED	
14	CHUKWUMA	ROMAN	SAVINGS	0012345614	PASSED	
15	IBOROMA	EMMANUEL	SAVINGS	0012345615	PASSED	
16	OLUMIDE	AYOMIDE	SAVINGS	0012345616	PASSED	
17	OLABISI	MICHAEL	SAVINGS	0012345617	PASSED	
18	AFOLABI	OSAS	SAVINGS	0012345618		FAILED
19	OMOREGIE	BLESSING	SAVINGS	0012345619		FAILED
20	DANIELS	VICTORY	CURRENT	0012345620	PASSED	

4.2 Results

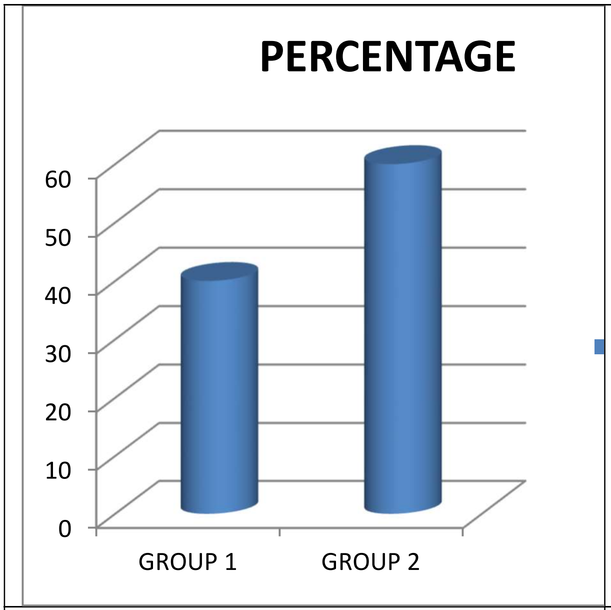
Based on the above procedure twenty (20) account users were allowed to use the Adaptive Data Mining and Intelligent Agent Framework for Credit Card Fraud Detection application and transactions processed ten (10) times in Table 4.1. With the use of generated tokens, they recorded levels of passes and failures during transaction processes for Credit Card Fraud Detection (CCFD) are given in Table: 4.2.

Table 4.2: Number of Passes and failures for ten (10) attempts

S/N	ACCOUNT NUMBER	CCFD PASSES	CC FD FAILED
1	0012345601	9	1
2	0012345602	8	2
3	0012345603	9	1
4	0012345604	7	3
5	0012345605	6	4
6	0012345606	7	3
7	0012345607	3	7
8	0012345608	4	6
9	0012345609	5	5
10	0012345610	9	1
11	0012345611	5	5
12	0012345612	8	2
13	0012345613	9	1
14	0012345614	7	3
15	0012345615	8	2
16	0012345616	9	1
17	0012345617	9	1
18	0012345618	7	3
19	0012345619	8	2
20	0012345620	7	3

Table 4.3: Percentage summary of passes from users

Range of Passes	No of Passes	Percentage
1-5(GROUP 1)	4	40
6-10 (GROUP2)	6	60



	PERCENTAGE
GROUP 1	40
GROUP 2	60

Fig 4.1: Graphical representation of passes on CCFD

Table 4.4 Percentage summary of Failures from users

Range of Failures	No of Failures	Percentage
1-5	5	71
6-10	2	29

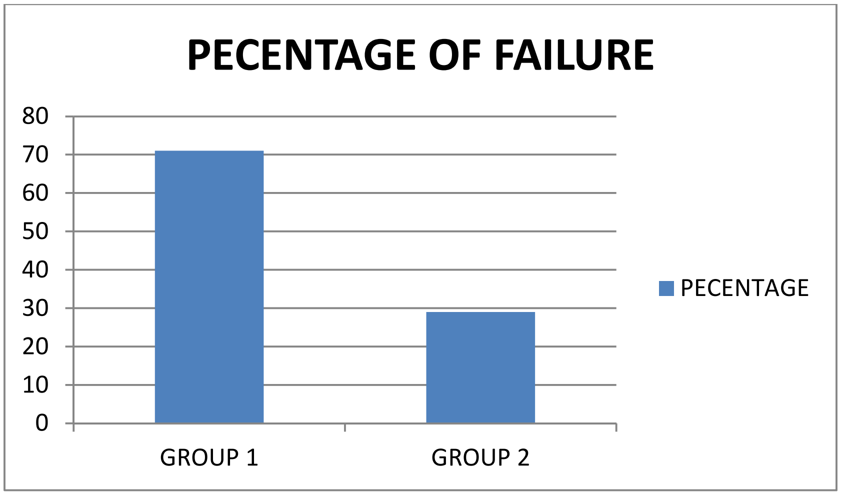


Fig 4.2 Graphical representation of failures on CCFD

5. CONCLUSION

This paper demonstrates the agent based technology development approach for detection of suspicious events in a financial transaction activity. The fraud detection system using adaptive data mining and intelligent agents' technology is an event driven transaction process for the financial institutions to enable them performs zero-trust check to determine any suspicious anomaly involved in accounts and to prevent data manipulation or even user assumption on key aspects of user accounts that could lead to fraud. Areas of application could range from banks, super stores, online shopping platforms, payment platforms to the database servers in other to check the spending profile of the card holders for the sole purpose of detecting credit card fraud.

REFERENCES

1. Alessandro, B. (2012). "Fraud Detection in the banking Sector. A multi-agent Approach. FTRA International Conference on 26-28.
2. Adekanye, F (2008) "Fraud in Banking Transactions". The Nigeria Bankers Volume 2nd Edition.
3. Akoroda, G.C.O (2004): "Frauds and Forgeries" WAJFEM Refiner course on Banking Supervision, Lagos.
4. Aleskerov, E, Fieisleben B and Bharat R (1997), "CARDWATCH: A Neural Network Based Database Mining System for Credit Card Fraud Detection," *Department of Electrical Engineering and Computer Science, University of Siegen,* pp 220-226.
5. Anuar, N.., Sallehudin H, Gani A and Zakari O,(2008). Identifying false alarm for network intrusion detection system using hybrid data mining and decision tree. Malaysian J. Comp. Sci., 21: 110-115.
6. Adepoju, A.S & Alhassan, M.E. (2010). Challenges of Automated Teller Machine (ATM) usage and fraud occurrences in Nigeria – A case study of selected banks in Minna metropolis. Journal of Internet Banking and Commerce. 15(2) 1-10.
7. Bolton,, R and Hand D (2002). "Unsupervised Profiling Methods for Fraud Detection," London.
8. Bolton, R. & Hand, D. (2012). 'Statistical Fraud Detection: A Review'. *Statistical Science.*
9. Brause R. Langsdorf T and Hepp M (2008). ''Credit Card Fraud Detection by Adaptive Neural Data Mining'. 1. W. Goethe-University, Comp. Sc. Dep. Report 7/99, Frankfurt
10. Chiu.C.. and Tsai. C. (2014). A Web Services-Based Collaborative Scheme for Credit Card Fraud Detection. Proceedings of IEEE international conference c-technology, c-commerce and e-service.
11. Cho B and . Park H (2013). "Efficient Anomaly Detection by Modeling Privilege Flows Using Hidden Markov Model," Computer and Security, 22(1) 45-55.
12. Chen, R. Chiu M., Huong Y and Chen L (2004). "Detecting Credit Card Fraud by Using Questionnaire. Responded Transaction Model Based on Support Vector Machines'. 800-806.
13. Costa, G., Folino F., Locane, A., Manco, G. and Ortale, R. (2007). Data mining for effective risk analysis in a bank intelligence scenario. Proceedings of the 23rd International Conference on Data Engineering Workshop, Apr. 17-20, IEEE Xplore Press, Istanbul, 904-911.
14. Chopra, B. Bhambri, V. Krishnan B, (2011). Implementation of data mining techniques for strategic CRM issues. Int. J. Computer. Tech. App., 2: 879-883.
15. Dheepa, V. and Dhanapal R, (2009). Analysis of credit card fraud detection methods. Int. J. Recent Trends Eng.,2: 126-128.
16. Delamaire L, Hussein A, John P (2009), "Credit card fraud and detection techniques: a review," *Banks and Bank Systems,* 4(2) 57-68.
17. Egu, .J. (2008): "The Role of Information and Communication Technology (ICT) in Fraud Detection in Nigerian Banks".
18. Ghosh S and . Reilly D (2014). ''Credit Card Fraud Detection with a Neural-Network,'' Proc. 27th Hawaii Int'l Conf. System Sciences: Information Systems: Decision Support and Knowledge-Based Systems. 3 621-630.
19. Huang X,. Hu, J and Bertok. P (2007). "A Multi- Layer Model for Anomaly Intrusion Detection Using Program Sequences of System Calls," Proceedings of 11th IEEE Int'l Conf. Network. 531-536
20. Hand, D. (2007). Statistical techniques for fraud detection, prevention, and evaluation'', Imperial College London.
21. Hand, D. (2010). "Fraud Detection in Telecommunications and Banking: Discussion of Becker.
22. He, J., Zhang, Y, Shi .Y and . Huang G, (2010). Domain-driven classification based on multiple criteria and multiple constraint-level programming for intelligent credit scoring. IEEE Trans. Knowledge. Data Eng., 22: 826-838. DOI: 10.1109/TKDE.2010.43

23. Ingle, D. and Meshram, B. (2012). E-Investment banking: NextGen investment. Int'l Journal of. Advanced Research in Computer, Engineering and Technology.
24. Joh, G.H. (2017). Hybrid approach for detecting credit card. 1st Journal ISSN 1468-0394 www.onlinelibrary.wiley.Tech.
25. Joshi , S and Phoha V (2014). 'Investigating Hidden Markov Models Capabilities in Anomaly Detection," Proc. 43rd ACM Ann. Southeast Regional Conf. 1 98-103
26. Jiawen, H, Micheline K, and Jian P (2011). "Data Mining: Concepts and Techniques", 3rd edition, the Morgan Kaufmann Series. 244-254.
27. Kazi, I. Baseer, A. (2012). "Use of Data Mining in Banking" International Journal of Engineering Research and Applications 2(2) 38-42.
28. Koru (2014): "Real time Multi-Agent Based Fraud Detection Tool for banking institutions.
29. Khan M, Jahir P. Ali H, Ekbal A (2014). "Credit Card Fraud Detection System Using Hidden Markov Model and K-Clustering". International Journal of Advanced Research in Computer and Communication Engineering 3(2).
30. Kim, M.J. and Kim, T.S. (2010). "A Neural Classifier with Fraud Density Map for Effective Credit Card Fraud Detection," Proc. Int'l Conf. Intelligent Data Eng. and Automated Learning
31. Khac, N. . Markos S, . Brabazon A and M. Kechadi, (2011). An investigation into data mining approaches for Anti-Money Laundering. Proceedings of the International Conference on Computer Engineering Applications, (EA* 11), Lacsit Press, Singapore, 504-508.
32. Li, W. and Liao. J,(2011). An empirical study on credit scoring model for credit card by using data mining technology. Proceedings of the 7th International Conference on Computational Intelligence and Security, Dec. 3-4, IEEE XplorPress, Hainan, 1279-1282.DOI: 10.1109/CIS.20U.283
33. Laleh N and , Azgomi A (2009). "A Taxonomy of Frauds and Fraud Detection Techniques," *ICISTM,* 31, 256-267.
34. Margaret, R. (2014). http://www.searchsecurity.techtarget.com/definition/tw o-1factor-authentication.
35. Massimilliano, Z., Miguel, R. and Santiago, M. (2018): credit card fraud detection through Parenclitic Network Analysis. Complexity 2018 article ID:5764370 https://doi.org//l0.1155/2018/5764370.
36. Ngai, E, . Xiu L and Chau D,(2009). Application of data mining techniques in customer relationship management: A literature review and classification. Expert Syst. App.36: 2592-2602. DOI: 10.1016/j.eswa.2008.02.021
37. Naeini, M., Taremian H and Hashemi H, (2010). Stock market value prediction using neural networks. Proceedings of the International Conference on Computer Information Systems and Industrial Management Applications, Oct. 8-10, IEEE Xplore Press, Krackow, 132-136.
38. Ogwueleka F. (2011). "Data mining application in Credit Card Fraud Detection System" Journal of Engineering Security and Technology. 6(3) 311-322.
39. Ovuakporie, V, (1994): "Bank Frauds: Cause and Prevention-An empirical analysis, Ibadan, ATT Book Ltd. 23.
40. Priyaka, Y,Pavan W, Manish T (2016). "Proposal distributed data mining in Credit Card Fraud Detection International research journal of engineering and Technology.
41. Patidar, R and Sharma L (2011). "Credit Card Fraud Detection Using Neural Network," *International Journal of Soft Computing and Engineering (IJSCE),* 1(2) 2231-2307.
42. Patidar, R,and Lokesh S (2011). "Credit Card Fraud Detection using Engineering (IJSCE), 1(2).
43. Phua, C., Lee, V., Smith, K. & Gayler, K (2014). A comprehensive survey of data mining-based fraud detection research, Artificial Intelligence Review 1-14.

44. Ping, Z. and Liang S, (2010). Data mining application in banking-customer relationship management. Proceedings of the International Conference on Computer Application and System Modeling. IEEE Xplore Press, Taiyuan, 124-126.
45. Qiu, D., Q. Wang, Y. and Zhang, (2009). A mode for a bank to identify cross-selling opportunities. Proceedings of the International Conference on Computational Intelligence and Software Engineering. IEEE Xplore Press, Wuhan, 1-4.
46. Ren, S. and Shy, D. (2010). Customer segmentation of bank based on data warehouse and data mining. Proceedings of the 2nd IEEE International Conference on Information Management and Engineering. IEEE Xplore Press, Chengdu, 349-353.
47. Ratha, N.K. and Bolle R.M., (2014). "Smart card based Authentication," *IBM Systems Journal,* retrieved from http://www.cse.msu.edu/~cse891/Sect601/textbook/18.
48. Saravanan, S.K. and Suresh, B. (2017). An Improving Credit Card Fraud Detection using a Novel Data Technique. India Research Organization. ISSN2394-0697 Vol 4.
49. Stolfo, S., Fan,W. Lee, A. (2010). "Credit Card Fraud Detection Using Meta-Learning: Issues and Initial Results," Proc. AAAI Workshop AI Methods in Fraud and Risk Management, 83-90.
50. Sharraa, A, Panigrahi P,(2012). A review of financial accounting fraud detection based on data mining techniques. International journal. J. Computer. Application, 39: 37-47
51. Tak-chung, F (2011). A review on time series data mining. Eng. Applied Artificial Intelligence. 164-181.
52. Varun, K., Chaitanya, V. and Madhavan, M. (2012). Segmenting the banking market strategy by clustering. International Journal in Computer Application.
53. Wikipedia, "Authentication," retrieved Oct 12, 2014 http://en.wikipedia.org/wiki/Authentication
54. Xiong T, Wang S, Mayers A and Monga E (2013), "Personal bankruptcy prediction by mining credit card data," *Expert Systems with Applications,* 665-676.