ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

Utilizing Area Mindful Business Principles for Anticipating Retail keeping money cheats

V.P.Gladis Pushparathi[1], B.Abishiek[2], C.H.Viswanathudu [3], C.S.Inbaswaran [4], A.Ashwin [5]

Associate Professor, Department of CSE, Velammal Institute of Technology, Chennai, Tamil Nadu, India[1]

U.G Students, Department of CSE, Velammal Institute of Technology, Chennai, Tamil Nadu, India [2, 3, 4]

ABSTRACT: The detection of fraud activities in national and international economies have become the important task. The security of transactions by banks and other financial institutions is one of the major factors affecting the reputation and profitability of such organizations. It is more difficult to catch a person, who does fraudulent transactions. Detecting this type of transactions makes the support of technology compulsory, considering high volume and intensity of transactions. We propose a system for fraud detection and prevention system for retail banking. Depending on how much mobile the card owners are, we can easily devise business rules to detect the anomalies. Such anomalies can be directed to appropriate business units to be analyzed further or account owners may be required additional authorizations for banking activities. The proposed system is used to analyze the every details of the user transaction and detect the fraudulent activities.

I. INTRODUCTION

Money laundering (ML) refers to the use of multiple financial proceeds to cover up the illegal source of funds from corruption, fraud and other forms of crime, making the money appear legitimate. With the increasing rampant of upstream crime, ML is posing a more serious threat to financial institutions as well as national security. How to effectively detect abnormal financial activities has become a huge challenge faced by governments and financial institutions. Some anti-money laundering (AML) systems have been deployed to combat with criminals. Nevertheless, most AML systems are still rule-based, suffering from numerous of drawbacks such as lack of pattern recognition function and easy to be avoided.

II. MONEY LAUNDERING & ANTI MONEY LAUNDERING

Money laundering is the generic term used to describe the process by which criminals disguise the original ownership a And control of the proceeds of criminal conduct by making such proceeds appear to have derived from a legitimate source. The processes by which criminally derived property may be laundered are extensive. Though criminal money may be successfully laundered without the assistance of the financial sector, the reality is that hundreds of billions of dollars of criminally derived money is laundered through financial institutions, annually. The nature of the services and products offered by the financial services industry (namely managing, controlling and possessing money and property belonging to others) means that it is vulnerable to abuse by money launderers. If you're considering developing your career in anti-money laundering, find out more about joining ICA's global community here. Becoming a member today will give you access to a wealth of knowledge, tools, resources and practical support to help develop your career. Being a member of ICA also demonstrates a commitment to the highest standards of practice and conduct and enhances your professional reputation and employability.

Anti-money laundering (AML) refers to a set of procedures, laws and regulations designed to stop the practice of generating income through illegal actions. Though anti-money-laundering laws cover a relatively limited number of transactions and criminal behaviors, their implications are far-reaching. For example, AML regulations require institutions issuing credit or allowing customers to open accounts to complete due-diligence procedures to ensure they are not aiding in money-laundering activities. The onus to perform these procedures is on the institutions, not on the criminals or the government.

DOI: 10.15680/IJIRCCE.2019. 0702111

Objective:
A comprehensive method for detecting suspicious ML gangs in massive transaction networks has been presented. Noise information is filtered out first to reduce the total computation cost. An algorithm incorporated with rich AML experience has been proposed to detect communities. The algorithm has also been parallelized and optimized in Spark platform, which was applied to deal with the massive real transaction data. At last, the most suspicious ML communities can be picked out by reordering the calculated risk score. This solution has been proved to be a powerful auxiliary tool for monitoring department carrying out anti-money laundering work.

III. LITERATURE SURVEY

Title:
Intelligent Anti-Money Laundering System
Author:
S. GAO, D. Xu, H. Wang and Y. Wang
Abstract:
Criminal elements in today's technology-driven society are using every means available at their disposal to launder the proceeds from their illegal activities. While many anti-money laundering solutions have been in place for some time within the financial community, they cannot adapt to the ever-changing risk and methods in relation to money laundering. In order for a more adaptive, intelligent and flexible solution for anti-money laundering, the intelligent agent technology is applied in this research. Intelligent agents with their properties of autonomy, reactivity and proactivity are well suited for money laundering prevention controls. Several types of agents are proposed and a novel and open multi-agent architecture is presented for anti-money laundering. A prototype system for money laundering detection is also developed to demonstrate the advances of the proposed system architecture and business value.
Paper 2:
Title:
Application of Data Mining for Anti-Money Laundering Detection: A Case Study
Author:
N. Khac and M. Kechadi
Abstract:
Recently, money laundering is becoming more and more sophisticated; it seems to have moved from the personal gain to the cliché of drug trafficking and financing terrorism. This criminal activity poses a serious threat not only to financial institutions but also to the nation. Today, most international financial institutions have been implementing anti-money laundering solutions but traditional investigative techniques consume numerous man-hours. Besides, most of the existing commercial solutions are based on statistics such as means and standard deviations and therefore are not efficient enough, especially for detecting suspicious cases in investment activities. In this paper, we present a case study of applying a knowledge-based solution that combines data mining and natural computing techniques to detect money laundering patterns. This solution is a part of a collaboration project between our research group and an international investment bank.

Proposed System

We explore practicality of using location data to aid finding better business rules where they can easily be deployed with a rule-based fraud detection and prevention system for retail banking. This rule-based fraud detection system is implemented by using a unique identification key for online purchases. By using that key, the user will be tracked in the purchases, the number of accounts and the various amounts of transactions he is making. Fraud detection activities involves monitoring the behavior of transactions and prevention means a proactive approach that involves the analysis of transactions before they completed and identifying if they are fraud or not . In highly connected societies that we now live in, financial fraud is very common to the point that financial institutions form various business units to guard their customers, capital and infrastructure as well as their reputation. Fraud cases involve criminal purposes and they are very hard to identify in most cases. As new application channels increase in use (e.g., mobile), new fraud opportunities present themselves, and anonymity becomes easier. The issue is that if financial institutions' fraud detection tools remain static, they can be exploited by the fraudsters who quickly identify thresholds and take advantage.

Financial fraud is composed of bank fraud, securities and commodities fraud, insurance fraud and other related financial frauds. Detecting financial fraud is very crucial for preventing often large scale. The activities of the user will be tracked and the suspicious transactions alone will be reported for any threat. In order to study the importance of location data, we first compiled a set of anonym zed automated teller machine usage data from a mid-size bank in Turkey. Ensuring the security of transactions carried out by banks and other financial institutions is one of the major factors affecting the reputation and profitability of such organizations. However, since people who perform fraudulent transactions change their methods constantly in order not to get caught up, it gets more difficult to identify and detect this type of transactions. Detecting this type of transactions makes the support of technology compulsory, considering high volume and intensity of transactions. Depending on how much mobile the card owners are, we can easily devise business rules to detect the anomalies. Such anomalies can be directed to appropriate business units to be analyzed further or account owners may be required additional authorizations for banking activities (such as internet money transfers and payments). We have shown in this paper that a significant bulk of users does not leave the vicinity of their living place. We also give some brief use cases and hints regarding what types of business rules can be extracted from location data.

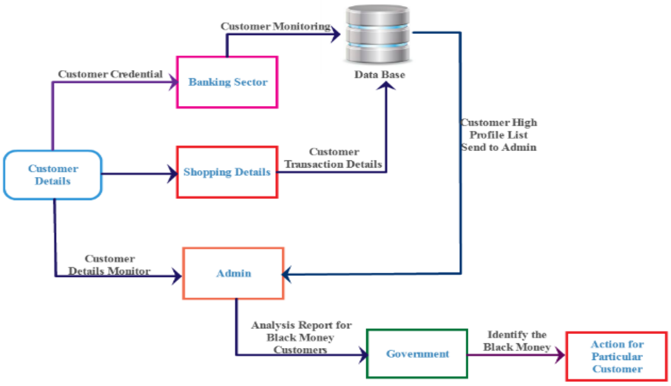
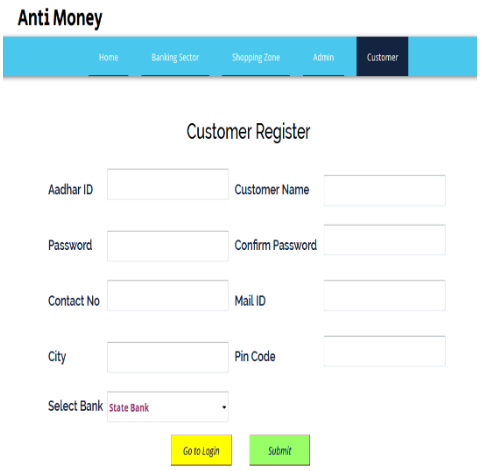


fig 1.1 Architecture Diagram

IV. RESULTS

Customer Identification Requirements:

An Authorized Firm should adopt a risk-based approach for the customer identification and verification process. Depending on the outcome of the Authorized Firm's money laundering risk assessment of its customer, it should decide to what level of detail the customer identification and verification process will need to be performed.



Select Bank: State Bank

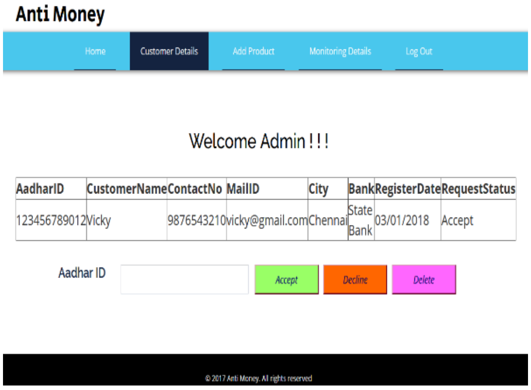
fig 1.2 Customer Registration

Internal & External Reporting Requirements:

The requirement for Employees to make an internal Suspicious Transaction Report should include situations when no business relationship was developed because the circumstances were suspicious. In preparation of an external Suspicious Transaction Report, if an Authorized Firm knows or assumes that the funds which form the subject of the report do not belong to a customer but to a third party, this fact and the details of the Authorized Firm's proposed course of further action in relation to the case should be included in the report.

Government Findings:

An authorized Firm must establish and maintain systems and controls to obtain and make appropriate use of any findings, recommendations, guidance, directives, resolutions, sanctions, notices concerning arrangements for preventing money laundering or terrorist financing in a particular country or jurisdiction, including any assessment of material deficiency against relevant countries in adopting international standards.

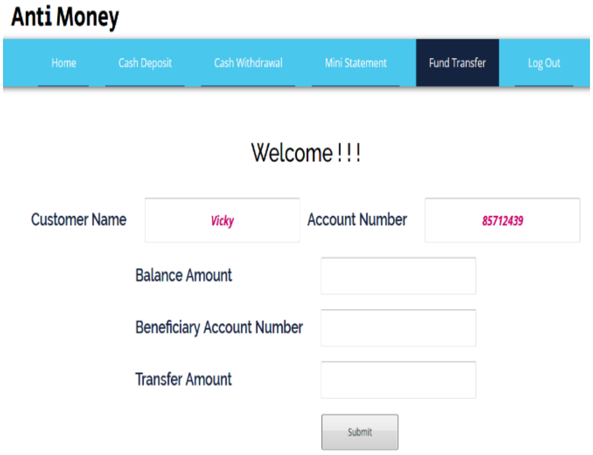


AadharID	CustomerName	ContactNo	MailID	City	Bank	RegisterDate	RequestStatus
123456789012	Vicky	9876543210	vicky@gmail.com	Chennai	State Bank	03/01/2018	Accept

fig 1.3 Admin access

Transfer of Funds:

Where an authorized Firm is a financial institution and makes a payment on behalf of a customer to another financial institution using an electronic payment and message system, it must include the customer's name, address and either an account number or an unique reference number in the payment instruction.



Customer Name Vicky Account Number 85712439

Balance Amount

Beneficiary Account Number

Transfer Amount

fig 1.4 Fund Transfer

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

V. CONCLUSION

In this paper, we presented a sophisticated solution to find transfer communities with high ML risks in massive transaction networks. Firstly, a whole transaction graph is built by merging edges. The next, transfers with less ML possibility are filtered out by selecting suspicious MLSs. Then combined with AML patterns is proposed and implemented on remaining MLSs. The further divided into different communities with their ML risk scores calculated. Finally, MLSs containing multi communities at high risk levels are further investigated and reported. The results demonstrate that our solution can help to find out criminal gangs with high ML risks in massive transaction networks efficiently and intelligently.

FUTURE ENHANCEMENT

The proposed system aims on monitoring the user money transaction and the details of the user is being tracked , In future we aims to enhance the system to block the amount illegally transferred and makes the user not to access the money till the clearance is confirmed by the user. This enhancement will make the abrupt block of black money being accessed.

REFERENCES

1. P. D. Meo, E. Ferrara, G. Fiumara, and A. Provetti, “Generalized louvain method for community detection in large networks,” IEEE International Conference on Intelligent Systems Design and Applications, vol.79, p. 88-93, 2012.
2. Y. Liu, F. Chen, W. Kong, H. Yu, M. Zhang, S. Ma and L. Ru, “Identifying web spam with the wisdom of the crowds,” Acm Transactions on the Web, vol. 6, p. 1-30, 2012.
3. X. Que, F. Checconi, F. Petrini and J. A. Gunnels, “Scalable community detection with the louvain algorithm,” IEEE International Parallel and Distributed Processing Symposium, p. 28-37, 2015.
4. N. Dugué, A. Perez, “Directed Louvain: maximizing modularity in directed networks,” Research Report, Université d’Orléans, 2015.
5. C. Wickramaarachchi, M. Frincu, P. Small and V. K. Prasanna, "Fast parallel algorithm for unfolding of communities in large graphs," IEEE High Performance Extreme Computing Conference, pp. 1-6, 2014.
6. SreekumarPulakkazhy and R.V.S.Balan,”Data Mining in Banking and its applications –A Review”, Journal of computer science 2013.G.
7. G.Krishna priya,Dr.M.Prabakaran”Money laundering analysis based on Time variant Behavioral transaction patterns using Data mining”Journal of Theoretical and Applied Information Technology 2014.
8. Xingrong Luo,”Suspicious transaction detection for Anti Money Laundering”, International Journal of Security and Its Applications 2014.
9. Ch. suresh,Prof.K.Thammi Reddy,”A Graph based approach to identify suspicious accounts in the layering stage of Money laundering”,Global Journal of computer science and Information Technology 2015.
10. Denys A.Flores, Olga Angelopoulou, Richard J. Self,” Design of a Monitor for Detecting Money Laundering and Terrorist Financing”, International Journal of Computer Networks and Applications 2014.
11. Anu and Dr. Rajan Vohra,” Identifying Suspicious Transactions in Financial Intelligence Service”, International Journal of Computer Science & Management Studies July 2014.
12. Quratulain Rajput, Nida Sadaf Khan, Asma Larik, Sajjad Haider, “Ontology Based Expert-System for Suspicious Transactions Detection”, Canadian Center of Science and Education, Computer and Information Science; Vol. 7, No. 1, 2014.
13. Mahesh Kharote, V. P. Kshirsagar, “Data Mining Model for Money Laundering Detection in Financial Domain”, International Journal of Computer Applications (0975 – 8887), Volume 85 – No 16, 2015.
14. Harmeet Kaur Khanuja, Dattatraya S. Adane, “Forensic Analysis for Monitoring Database Transactions”, Springer, Computer and Information Science Volume 467, pp 201-210, 2016.
15. Pradnya Kanhere, H. K. Khanuja,” A Survey on Outlier Detection in Financial Transactions, International Journal of computer Applications, December2015.