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. 6, Issue 1, January 2018

Utilizing Business Principles for Anticipating Transaction to Prevent Money Cheats

S.Aravind Kumar[1], S.Paul Kingsley[2], R.Santhosh [3]

Assistant Professor, Department of Computer Science and Engineering, Jeppiaar SRR Engineering College, Padur, Tamil Nadu, India

B.E, Department of Computer Science and Engineering, Jeppiaar SRR Engineering College, Padur, Tamil Nadu, India

B.E, Department of Computer Science and Engineering, Jeppiaar SRR Engineering College, Padur, Tamil Nadu, India

ABSTRACT: Money Laundering [ML] alludes to the utilization of different monetary continues to conceal the illicit wellspring of assets from corruption/debasement, extortion and different types of wrong doing, profiting seem honest to goodness. With the expanding uncontrolled of upstream wrong doing, ML is representing a more genuine danger to money related foundations and national-security. Step by step instructions to viably identify unusual money related exercises has turned into an immense test looked by governments and monetary organizations. Anti-Money Laundering [AML] alludes to an arrangement of methodology; laws-and-controls intended to stop the act of producing pay through illicit activities. Despite the fact that hostile to Anti-Money-Laundering laws cover a moderately predetermined number of exchanges and criminal practices, their suggestions are expansive. Black Money reserves earned on the bootleg market, on which salary and different assessments have not been paid. Likewise, it is the unaccounted cash that is covered from the expense administrator. One of the critical methods to change over the black money to white cash is by making utilization of needy individuals as cash-mules utilizing their financial balances. It is harder to get a man, who does false exchanges nowadays. Identifying these kind of exchanges makes the help of innovation obligatory, thinking about high volume and power of exchanges. Contingent upon how the exchanges being made by the card proprietor every one of the oddities can be recognized utilizing against illegal tax avoidance system to anticipate the extortion exchange. Such oddities can be coordinated to proper specialty units to be broke down further or record proprietors might be required extra approvals for keeping bank activities. The proposed framework is intended to break down each detail of the client exchange to distinguish the deceitful activities and eliminate the money laundering events.

KEYWORDS: Money Laundering, ML, Anti-Money Laundering, AML, Black Money, Corruption.

I. INTRODUCTION

A comprehensive method for detection suspicious ML gangs in massive transaction network has been presented in this system. An algorithm incorporated with rich AML experience has been proposed to detect communities with high ML risks. The algorithm used in this system is Community detection Algorithm which is used 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.

DOI: 10.15680/IJIRCCE.2018. 0601074

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. 6, Issue 1, January 2018

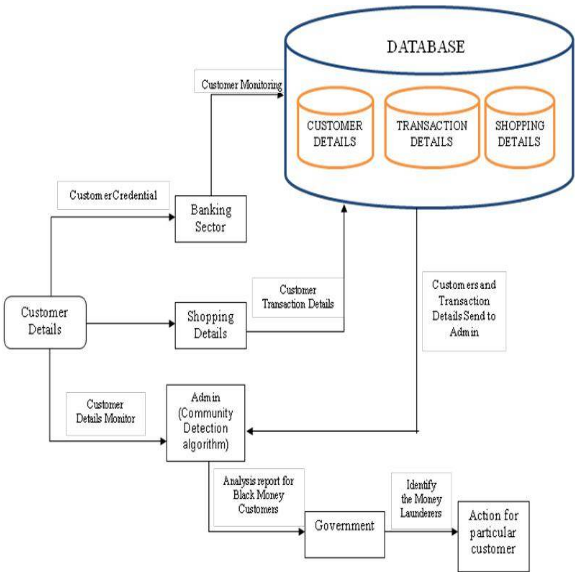
DATABASE
CUSTOMER DETAILS
TRANSACTION DETAILS
SHOPPING DETAILS
Customer Monitoring
CustomerCredential
Banking Sector
Customer Details
Shopping Details
Customer Transaction Details
Customers and Transaction Details Send to Admin
Customer Details Monitor
Admin (Community Detection algorithm)
Analysis report for Black Money Customers
Government
Identify the Money Launderers
Action for particular customer

Fig.1 Proposed System Architecture

between the two into national problem as social and economy are major component in defining stability and harmony of nation.

Money laundering is one of the most related derivatives of crimes involving money and it is said money laundering activities are being the most difficult crimes to cater and to control. Even though having a good constructed law by good legislature together with serious enforcement of the law, soft crimes like money laundering still difficult to trace. Dangerous invincible threats of the social and economic security plus difficult to trace crime like money laundering absolutely turns the relationship

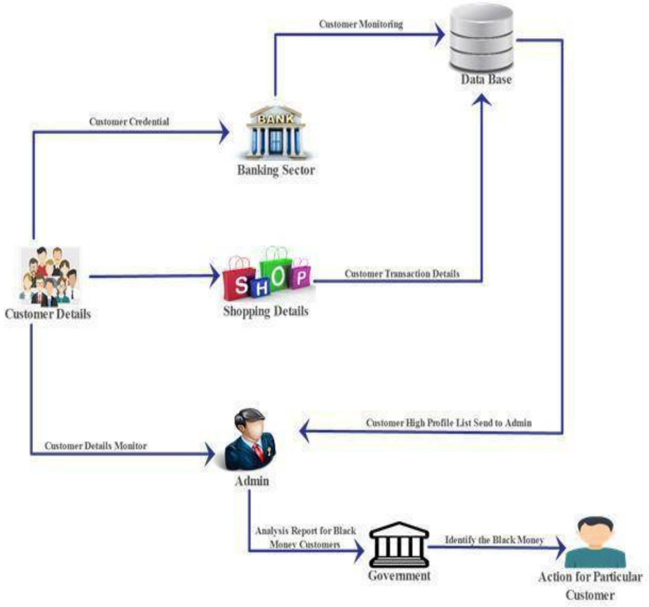

Fig.2 Functional Architecture of the Proposed System

II. PAST SYSTEM ANALYSIS

In the past system implementations, there are several difficulties in money laundering detection. People involved in money laundering obviously try to conceal the real purpose of money transfers used in this process. Therefore, one can expect that individual transactions will not clearly stand out from amongst other bank transfers. The probability of a fraud depends not only on parameters of individual bank transfer but also on relations with other transfers and the entities that send them. The volume and value of transactions reported as suspicious are very high.

For example, the value of transactions reported to the anti-money laundering watchdog by Russian financial institutions in the first nine months of 2010 was 120 trillion roubles. 5.6 million Filings were made by banks, insurance companies and financial service companies in this period. The past system contains many drawbacks over practical implementations, there as listed as follows:

(i) The perpetrators of criminal acts strive to make the transactions as innocent-looking as possible. It is never possible to identify all illegal activities.

(ii) Identifying Money Laundering is very difficult task due to vast number of transactions were involved.

(iii) This process is time consuming and not suitable to identify the illegal transactions that occurs in the system immediately.

III. PROPOSED SYSTEM SUMMARY

In the proposed system, by exploring the practicality of using transaction details to aid finding better business rules where they can easily be deployed with a rule-based fraud detection and prevention system in banking sectors. Depending on how the card owners use their money, business rules are devised to detect the anomalies. Hence every transaction including withdraw, deposits and other transaction made online are monitored continuously for any 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 approach has many advantages, they are listed as below:

(i) To identify the fraudulent transaction where a larger amount is split to smaller transfers in order to decrease the probability that individual transactions will be reported as suspicious.

(ii) The purpose of obscuring the connection between the sender and the receiver. The entire money laundering operation may involve many such schemes, so identification of a suspicious may help in uncovering much larger network of illegal transactions.

(iii) To identify Money laundering operations which are intertwined with many other transactions, including legal ones.

IV. COMMUNITY DETECTION ALGORITHM

The community detection algorithm can be powerful tool to divide these complex structures into more subdivided but meaningful groups. By calculating then suspicious degree for each group, the ML risk for the total complex transaction structures can be quantitatively described. On the other hand, transfer time and direction are two crucial factors during anti-money laundering processes. And the amount that's been transacted is an important asset in analyzing the result. Further complex ML crimes can be predicted and prevented if inherent evolution law of the transaction structure is grasped in early times.

V. CUSTOMER IDENTITY REQUIREMENT AND VALIDATION

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.

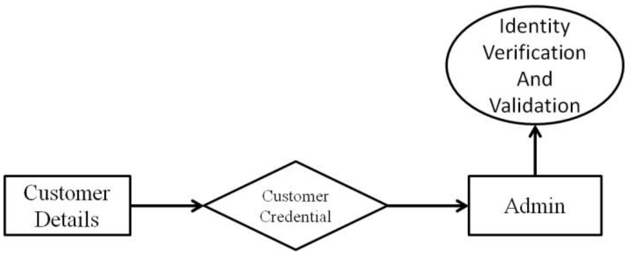

Fig.3 Customer Identity Requirement and Validation

Transfer of funds

To transfer money to another account or any 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.

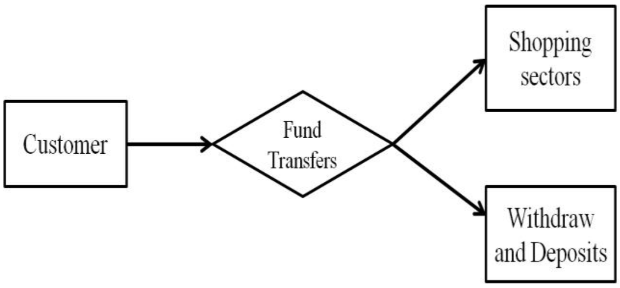

Fig.4 Transfer of Funds

Shopping

Admin has the rights to add products for the users to purchase online. In this way money spent on online shopping is also monitored , so that any bulk unaccounted money spent on online shopping can also be monitored by the admin . Black money spent on online shopping by purchasing products in bulk amount can be identified.

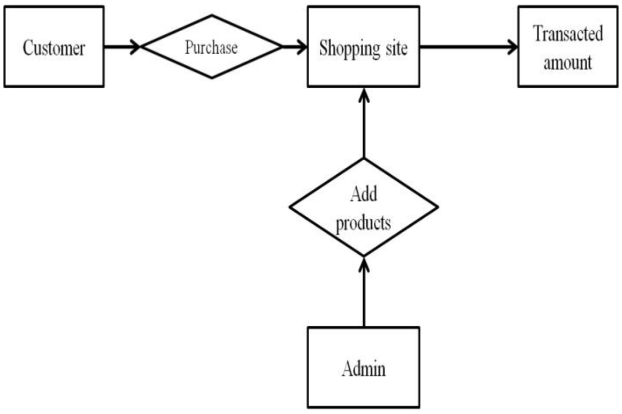

Fig.5 Shopping

Analysis Report

The System should generate a report corresponding to the result analyzed from the the transactions according to their ML risks .A Community Detection Algorithm is used to analyze the ML risk of the transaction. If any suspicious transaction is found a report is generated and it is forwarded to the authorized firm which establish and maintains a system to control and make appropriate use of our findings.

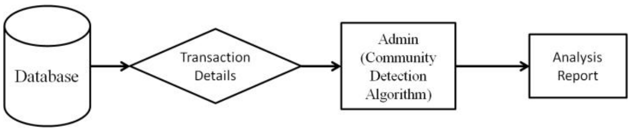

Fig.6 Analysis Report

VI. LITERATURE SURVEY

In the year of 2009, the authors "M. Ahmad, B. Keegan, J. Srivastava, D. Williams, and N. Contractor" proposed a paper titled "Mining for gold farmers: Automatic detection of deviant players in MMOGs", in that they described such as: Gold Farming alludes to the unlawful routine with regards to get-together and offering virtual merchandise in web based diversions for genuine cash. Despite the fact that around one million gold agriculturists take part in gold cultivating related exercises, to date a methodical investigation of recognizing gold ranchers has not been finished. In this paper, information are utilized from the greatly multiplayer online pretending diversion (MMORPG) EverQuest II to distinguish gold agriculturists.

An exploratory calculated relapse examination to recognize remarkable expressive measurements took after by a machine learning two fold grouping issue to distinguish an arrangement of highlights for order purposes. Given the cost related with exploring gold ranchers, we additionally give criteria for assessing gold cultivating identification procedures, and give proposals to future testing and assessment systems.

In the year of 2011, the authors "B. Keegan, M. Ahmed, D. Williams, J. Srivastava, and N. Contractor" proposed a paper titled "Sic transit gloria mundi virtuali?: Promise and peril in the computational social science of clandestine organizing", in that they described such as: MMOGs keep up chronicled databases of all player activities and traits including movement by accounts occupied with illegal conduct. On the off chance that people in online universes work under comparative social and mental inspirations and imperatives as the

disconnected world, online behavioral information could advise hypotheses about disconnected conduct. Looking at high hazard exchanging connections in a MMOG to light up the structures online covert associations utilize to adjust security with proficiency and contrast this with a disconnected medication trafficking system. This information offers the likelihood of performing social research on a scale that would be untrustworthy or impracticable to do in the disconnected world. Notwithstanding, investigating and summing up from undercover conduct in online settings brings up complex epistemological and methodological issues about the legitimacy of such mappings and what strategies and measurements are suitable in these unique situations. And finishing up by examining how computational sociology can be connected to on the web and disconnected criminological concerns and feature the "double utilize" ramifications of these innovations.

In the year of 2013, the authors "A. Kang, J. Woo, J. Park, and H. K. Kim" proposed a paper titled "Online game bot detection based on party-play log analysis", in that they described such as: as web based diversions wind up noticeably well known and the limit amongst virtual and genuine economies obscures, tricking in amusements has multiplied in volume and technique. In this paper, a structure for client conduct investigation for bot recognition in web based diversions is proposed. In particular, it is centered around party play which mirrors the social exercises among gamers: in a Massively Multi-client Online Role Playing Game (MMORPG), party play is a noteworthy movement that diversion bots endeavor to keep their characters safe and encourage the securing of digital resources in a manner altogether different from that of ordinary people. Through a thorough factual investigation of client practices in diversion movement logs, an edge levels are built up for the exercises that enable us to recognize amusement bots. In view of this, assemble a learning base of recognition rules, which are nonexclusive.

VII. CONCLUSION

In the proposed system , a sophisticated solution is presented to find transfer communities with high ML risks in massive transaction networks. Firstly, a whole transaction graph is built by merging edges. Then transfers with less ML possibility are filtered out by selecting suspicious transactions by using community detection algorithm. Then combined with Anti-money Laundering(AML) technique a patterns is proposed and implemented on remaining systems. The further divided into different communities with their ML risk scores calculated. Finally, transactions containing high money laundering risk levels are further investigated and reported. The results demonstrate that this solution can help to find out criminal gangs with high ML risks in massive transaction networks efficiently and intelligently.

REFERENCES

[1] Hyukmin Kwon, Aziz Mohaisen, Jiyoung Woo, Yongdae Kim, Eunjo Lee, Huy Kang KimC*, “Crime Scene Reconstruction: Online Gold Farming Network Analysis” ,IEEE Transactions on service computing, august 2017.

[2] E. Lee, J. Woo, H. Kim, A. Mohaisen, and H. K. Kim, “You are a game bot!: uncovering game bots in MMORPGs via self-similarity in the wild,” in Proc. Network and Distributed System Security Symposium (NDSS’16), 2016

[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] J. Blackburn, N., Kourtellis, J. Skvoretz, M. Ripeanu, and A. Iamnitchi, “Cheating in online games: A social network perspective,” ACM Transactions on Internet Technology, vol. 13, no. 3, pp. 9:1-9:25, 2014.

[7]Xingrong Luo,”Suspicious transaction detection for Anti Money Laundering”, International Journal of Security and Its Applications 2014.

[8] A. Kang, J. Woo, J. Park, and H. K. Kim, “Online game bot detection based on party-play log analysis,” Computers and Mathematics with Applications, vol. 65, no. 9, pp.1384-1395, 2013.

[8] H. Kwon, K. Woo, C. H. Kim, C. Kim and H. K. Kim, “Surgical strike: A novel approach to minimize collateral damage to game BOT detection,” in Proc. Annual Workshop on Network and Systems Support for Games, 2013, pp.1-2.

[9] J. Woo, A. Kang, and H. K. Kim, “The contagion of malicious behaviors in online game,” Computer Communication Review, vol. 43, pp. 543-544, 2013.

[10] A. Kang, H. K. Kim, and J. Woo, “Chatting pattern based game bot detection: Do they talk like us? ,” KSII Transactions on Internet & Information Systems, vol. 6, pp. 2866-2879, 2012.

[11] B. Keegan, M. A. Ahmad, D. Williams,J.Srivastava, and N.Contractor, “What can gold farmers teach us about criminal networks?,” XRDS: Crossroads, The ACM Magazine for Students, vol. 17, no. 3, pp. 11-15, 2011.

[12] B. Keegan, M. Ahmed, D. Williams, J. Srivastava, and N. Contractor, “Sic transit gloria mundi virtuali?: Promise and peril in the computational social science of clandestine organizing,” in Proc. 3rd International Web Science Conference (WebSci ’11), 2011.

[13] K. Woo, H. Kwon, H. Kim, C. Kim, and H. K. Kim, “What can free money tell us on the virtual black market?” Computer Communication Review, vol. 41, no. 4, pp. 392-393, 2011.

[14] M.J. Newman, "Networks: An introduction." Oxford University Press, 2010.

[15] D. Easley, and J. Kleinberg. Networks, Crowds, and Markets: Reasoning About a Highly Connected World, Cambridge University Press, 2010.

[16] S. Gianvecchio, Z. Wu, M. Xie, and H. Wang, “Battle of botcraft: Fighting bots in online games with human observational proofs,” in Proc. 16th ACM conference on Computer and Communications Security, 2009, pp. 256-268.

[17] S. Mitterhofer, C. Platzer, C. Kruegel, and E. Kirda, “Server-side bot detection in massive multiplayer online games,” IEEE Security and Privacy, vol. 7, no. 3, pp. 29-36, 2009.

[18] R. Thawonmas, Y. Kashifuji, and K. Chen, “Detection of MMORPG bots based on behavior analysis,” in Proc. 2008 International Conference on Advances in Computer Entertainment Technology, 2008, pp. 91-94.

[19] K. Chen, and L. Hong, “User identification basedon game-play activity patterns,” in Proc. 6th ACM SIGCOMM Workshop on Network and System Support for Games, 2007, pp. 7-12.

[20] S. Gao, D. Xu, H. Wang and Y.Wang, “Intelligent Anti-Money Laundering System," IEEE International Conference on Service Operations and Logistics, and Informatics, pp. 851-856, 2007.