INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 4, Issue 1)
Available online at www.ijariit.com

Literature Review on Diverse Techniques in Anti-Money Laundering System

A. Helen
helencanute@gmail.com
Easwari Engineering College, Chennai, Tamil Nadu

S. Sobitha Ahila
sobitha.ooviya@gmail.com
Easwari Engineering College, Chennai, Tamil Nadu

A. Niranjana
nithu6289@gmail.com
Easwari Engineering College, Chennai, Tamil Nadu

ABSTRACT

Money laundering is a process of converting black money into white cash. Anti-money laundering is a procedure or method to find these laundering activities. Although efforts on anti-money activities started at an early stage, the solutions seem to be restricted to a strategic level. Mostly the perpetrators of criminal acts strive to make the transactions as innocent looking as possible. Extensive research has been conducted to investigate a proper solution for suspicious transaction detection. But there is no reliable system to confirm if the exchange is really suspicious or not and the process is also very tedious. This paper surveys several approaches and algorithms that have been proposed for anti-money laundering System.

Keywords*: Anti Money Laundering, AROMLD, Bitcoin, Bitmap Index-based Decision Tree.*

1. INTRODUCTION

Money laundering is a process of converting unaccountable money into accountable money. Day to day the technology is getting updated and in this fast-changing technology, many merits as well as demerits, are associated. With the advent of E-Commerce, the world has been so globalized and further the technology has made everything so user-friendly that with a single click of a button, many transactions can be performed. Fraud Detection is mandatory since it affects not only to the financial institution but also to the entire nation. This criminal activity is appearing more and more sophisticated and perhaps this might be the major reason for the difficulty in fraud detection. This criminal activity leads to various adverse effects ranging from drug trafficking to financial terrorism.

Anti-money laundering is a process of finding the conversion of black money into white cash. In most cases, money launderers cover their actions through a series of steps that make it look like money coming from illegal or unethical origin was earned legitimately. Anti-money laundering software is a type of computer module used by financial institutions to review customer data and detect suspicious transactions. Anti-money laundering systems refine customer data, label it according to the level of suspicion and inspect it for anomalies. Such anomalies would include any immediate and substantial rise in funds or a large withdrawal. Smaller transactions that meet certain criteria may be also are fixed as suspicious.

2. ANTI-MONEY LAUNDERING IN ONLINE TRANSACTION

Kannan.S et al. (2017) [7], proposes the Autoregressive-based Outlier algorithm to minimize the computational complexity in the detection of ML activities (AROMLD). The Inter Quartile Range (IQR) estimation provides the variability measure for unknown values of the dataset. The successive computations of mean, zero mean, and regression deviation in proposed algorithm detects the ML actions in real-time financial systems with less time complexity.

Vikas Jayasree et al. (2017) [16], estimates the risk of money cleansing using Bitmap Index-based Decision Tree (BIDT) technique. Initially, the Bitmap Index-based Decision Tree learning is used to induce the knowledge tree which helps to determine a company's money laundering risk and improve scalability. In a BIDT bitmap index, the account in a table is numbered in sequence with each key value, account number, and a bitmap used. Subsequently, BIDT algorithm uses the “select” query performance to apply count and bit-wise logical operations on AND. Query result corresponds exactly to build a decision tree and more exactly to evaluate the adaptability risk in the money cleansing work. For the root node, the main account of the decision tree, the population frequencies

are obtained by simply counting the total number of "1" in the bitmaps constructed on the aspect to look for money laundering and estimate the risk factor rate. The experiment is conducted on factors such as regulatory risk rate, false positive rate, and risk identification time. The resulting analysis of BIDT technique using Statlog German Credit Data is compared with existing Smart Card-based Security Framework (SCSF) and Multilayered Detection System (MDS).

Ch.Suresh et al. (2016) [1], the apprehensive accounts of the layering stage of the money cleanse process are found by generating frequent transactional datasets using Hash-based association mining. The generated recurring datasets will then be used in the graph-theoretic approach to finding the traversal path of the suspicious transactions. The issue is that only the frequent accounts are taken as the only criteria for finding out the suspicious transaction as there may be a case when the transaction does not occur frequently but even then they are illegal.

Denys A. Flores, Olga Angelopoulos (2014) [2], projected a purposive system for Anti Money Laundering which examines and reviews the transactions depending on various techniques. The link analysis is the signature technique which is used to make stronger the analyst belief. By combing the rule-based approach and risk-based approach the risk-based approach can achieve the customer profile and transaction risk score. The authors used the clustering module to decrease the false positive alarms that may fatigue the Money laundering investigators.

Saeideh Alimolaei (2015) [15], a large number of cyber-attacks have been focused on online banking systems, and these attacks are considered as a significant security threat. Banks or customers might become the victim of the most complicated financial crime, namely internet fraud. This investigation has developed a rational system that enables finding the user's strange behavior in online banking. Since the user's behavior is associated with uncertainty, the system has been developed based on the fuzzy theory. This enables it to find user behaviors and categorize suspicious behaviors with various levels of intensity. This expert system is optimistic to be used for improving e-banking services security and quality.

Krishnapriya, Dr.M.Prabakaran (2014) [9], proposed a time-variant advent using the behavioral patterns where the transaction logs are separated for various timing windows and build upon it they generated the behavioral patterns of the customer. By the proposed approach it not only identifies the suspicious accounts but also identifies the group accounts which are involved in money laundering. Xingrong Luo (2014) [17], proposed an organized outlook of the data mining, framework of anti-money laundering, and also a classification based algorithm to effectively detect suspicious transactions. Clearly, they consider the financial transactions as a data stream, and to construct a classifier based on a set of mined frequent rules. They have experimented on a simulated transaction dataset based on real-world banking activities to show the efficiency of the proposed system. Moreover, every suspicious account is combined with others in the form of suspicious transactions which tied to two various accounts.

Murad Mehmet et al. (2013) [12], proposed a risk model for money laundering that assigns a risk value for transactions being a part of a larger chain of transactions that may be a part of a money laundering scheme. They use social networks to connect missing links in potential transaction sequences. Taken together we can provide a financial sector independent risk assessment to submitted transactions. Money laundering evolution detection framework (MLEDF) uses sequence equivalence, case-based study, social network analysis, and complex event processing to connective fraudulent transaction trails. MLEDF has constituent to collect data, run them across business rules and evolution models, run detection algorithms and use social network analysis to connect potential participants. This is advantageous compared with risk models that do not assess the risk of being involved in MLS, especially, considering the factors of increasing risk scores of MLEDF entities.

Pankaj Richhariya et al. (2012) [14], the prospect on fraud detection is unsettled to rise and rapid escalation of E-commerce, cases of financial fraud unified with it are also intensifying which results in a trouncing of billions of dollars worldwide each year. They provided a comprehensive and review of different techniques like credit card fraud detection, online auction fraud, telecommunication fraud detection, and computer intrusion technique. The disadvantage of the intrusion detection system has poor portability because the system and its rule set must be specific to the environment being monitored.

Nhien An Le Khac et al. (2010) [13], proposes a data mining based result for examining transactions to find money laundering and recommended an inspecting process based on divergent data mining techniques such as Decision tree, genetic algorithm, and fuzzy clustering. These techniques were proposed for quick recognition of customers for the purpose of application of Anti-money laundering and there have also proposed an inspecting process based on clustering and neural network to notice suspicious cases in the context of money laundering. In order to sharpen the running time heuristics such as suspicious screening were applied.

3. ANTI-MONEY LAUNDERING IN GOLD FARMING

Gold farming is an important division of the virtual economy. Gold farming was first used to elaborate on economics inside online games because just like the real world, the imaginary world can contain confined resources that are subject to the laws of supply and demand. Gold farming broadens this opinion into the existent economy, however as it involves the casting of virtual goods and currency for authentic money. Professional gold farmers are players likely from poorer regions who play games an entire day and sell their obtained virtual goods in order to earn the same wage as much as (or even more than) what they might earn for real work.

Hyukmin Kwon et al. (2017) [5], they analyze the characteristics of the ecosystem of a large-scale massively multiplayer online role-playing games (MMORPG) and devise a method for detecting GFGs. They build a graph that characterizes virtual economy transactions and traces abnormal trades and activities. Their extract features from the trading graph and physical networks used by GFGs to find them in their totality. Using their structure, they provide suggestion to defend effectively against GFGs while not affecting the existing virtual ecosystem.

Gold farming groups (GFGs) are organizations that gather and distribute virtual goods for capital gain in the online game world Gold farmer detection methods have evolved over the years, and the literature on the problem can be classified into three generations of related works.

Gian Vechio (2009) [4], the first generation of such methods is signature-based and utilizes client-side bot detection such as antivirus programs or CAPTCHA-based techniques. However, the first generation of commercial products could be learned from reverse engineering. Also, methods using CAPTCHA are known to be user-unfriendly and contribute to user annoyance. Finally, solving CAPTCHA has generated a thriving business that uses mechanical Turks utilized by underground players.

Kang (2013) [6], the second generation of methods focused on data-mining techniques and used server-side bot detection systems, which focused mainly on distinguishing between a bot and a benign player by analyzing server-side log files. Such techniques are widely used commercially and are coupled with logging techniques and various data mining algorithms for highly accurate bot detection. However, making a variant of an existing bot that can generate new behavioral patterns to thwart an existing detection technique is very easy and heavily utilized by gold farmers. Moreover, this method targets gold farmers individually. Companies have less insight of who belongs to the same group, and GFGs fight banning by continuously creating new gold farmers, making current banning efforts ineffective.

Kwon (2013) [10], the third generation methods are a surgical strike policy. They can detect all industrialized GFGs by group assuming that members of a group have frequent interaction and abnormal patterns. Because GFGs have the goal of economic achievement, the trade network provides hints to identify GFGs. Their detected GFGs based on the analysis of trade patterns merely based on the free money ratio; however, we could not detect GFGs group by group. We classify the role of each character (gold farmers, merchants, and bankers) in the GFGs. Gold farmers only collect game goods and when a certain amount of game goods are collected and they give the game money to the banker and items to the merchant. The banker collects all game money from GFG characters and sells the game money for real money. The merchant collects items from the gold farmers and sells them for game money. The merchant gives money earned from the items to the banking characters.

4. ANTI-MONEY LAUNDERING IN BITCOIN

Bitcoin is the first widely adopted decentralized digital e-cash system. All Bitcoin transactions that include addresses of senders and receivers are stored in the public blockchain which could cause privacy problems. The Zerocoin protocol hides the link between individual Bitcoin transactions without adding trusted third parties. However, such an untraceable remittance system could cause illegal transfers such as money laundering.

Ken Naganuma et al. (2017) [8], proposes an auditable decentralized e-cash scheme based on the Zerocoin protocol. Their scheme allows designated auditors to extract link information from Zerocoin transactions while preventing other users including miners from obtaining it. Respecting the mind of the decentralized system, the auditor does not have other authorities such as stopping transfers, confiscating funds, and deactivating accounts. A technical contribution of our scheme is that a coin sender embeds audit information with a non-interactive zero-knowledge proof of knowledge (NIZKP). This zero-knowledge prevents malicious senders from embedding indiscriminate audit information, and they construct it simply using only the standard Schnorr protocol for discrete logarithm without zk-SNARKs or other recent techniques for zero-knowledge proof.

Eli Ben-Sasson et al. (2014) [3], constructs a complete ledger-based digital currency with solid privacy warrant. They result leverage novel advances in zero-knowledge Succinct Non-interactive Arguments of Knowledge (zk-SNARKs). First, they compose and construct decentralized anonymous payment schemes (DAP schemes). A DAP system capacitate users to directly pay each other confidentially the corresponding transaction shields the payment's origin, destination and transferred amount. Second, they construct Zerocash, a practical instantiation of our DAP scheme construction. The result is if transactions are less than 1 KB and take time of 6 ms to check orders of magnitude then they are more efficient than the less-anonymous Zerocoin and competitive with plain Bitcoin.

Malte Moser et al. (2013) [10], they provide a first systematic account of opportunities and limitations of anti-money laundering (AML) in Bitcoin, They start from the observation that Bitcoin attracts criminal activity as many say it is an anonymous transaction system. While this claim does not stand up to scrutiny, several services offering increased transaction anonymization have emerged in the Bitcoin ecosystem – such as Bitcoin Fog, BitLaundry, and the Send Shared functionality of Blockchain.info. In a series of experiments, they use reverse-engineering methods to understand the mode of operation and try to trace anonymized transactions back to our probe accounts. While Bitcoin Fog and Blockchain.info successfully anonymize they test transactions, we can link the input and output transactions of BitLaundry. Against the backdrop of these findings, it appears unlikely that a Know-Your-Customer principle can be enforced in the Bitcoin system. Hence, they sketch alternative AML strategies accounting for imperfect knowledge of true identities but exploiting public information in the transaction graph, and discuss the implications for Bitcoin as a decentralized currency. In the first experiment, they were able to find a connection between one output and one input. The second experiment did not reveal any connections. In the third experiment, the service directly used half of the input transaction to generate an output transaction. Although our sample is not very large, it suggests that this service does not provide very good anonymity. A reason for this could be a low usage of the service as well as a lack of technical measures to ensure that users do not receive their input coins back.

5. RESULTS AND DISCUSSION

Table 1. Discussion on Results

ALGORITHM/ APPROACHES/ TECHNIQUE USED	RESULT
Autoregressive based outlier algorithm	Average area under the curve- 0.83 Average running time- 2.1 sec Accuracy - 94.4%
Bitmap index based decision tree	Risk identification time: BIDT technique is 9-25% compared to SCSF and 13-60% compared to MDS. False Positive rate: BIDT technique is 7-26% compared to SCSF and 19-55% compared to MDS. True positive rate: BIDT technique is 8-14% compared to SCSF and 12-21% compared to MDS.
Hashing Technique	When the no of transactions in the data set to rise, the no of frequent account also raise.
Classification based algorithm	Out of all 100 millions of transactions, they detected 317 accounts labeled as suspicious.
Money laundering evolution detection framework	The Rate is less than 5% and that is adequate considering the large transactions set.
Fuzzy expert systems	Accuracy- 94%

6. CONCLUSION AND FUTURE ENHANCEMENT

In this paper the anti-money laundering, it is a complex and difficult task. It is not easy to detect anomalous from the mass financial transaction. The various ways to launder the money like online transaction, gold farming and bitcoin and their techniques are done a detailed survey. The issues detected are as follows, the distribution of fragmented nodes was not more structured, difficult in handling voluminous financial institutions and consumption of time is more and the analyzed account is repeated each time even after the start of a new process.

In future instead of considering only the frequent accounts which are involved in the transaction, each and every account should be taken into account for investigating whether they are used frequently or not. They can also able to find the suspicious activities with less effort and time taken to include enhanced technologies.

7. REFERENCES

[1] Ch.Suresh, Dr.K.Thammi Reddy, N.Sweta,"A Hybrid Approach For Detecting Suspicious Accounts in Money Laundering Using Data Mining Techniques", *I.J Information Technology and Computer Science,* 2016,vol. 5,pp. 37-43, 2016.

[2] 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.

[3] Eli Ben-Sasson, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, Madars Virza, "Zerocash: Decentralized Anonymous Payments from Bitcoin", *IEEE,* pp. 459-474, 2014.

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

[5] Hyukmin kwon, Aziz mohaisen, Jiyoung wow, Yougdae kim, Eunjo lee, Hug kang lee, "Crime Scene Reconstruction: Online Gold Farming network analysis", *IEEE Transactions on service computing,* Aug. 2017.

[6] 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.

[7] Kannan s, Somasundaram k, "Autoregressive based outlier algorithm to detect money laundering activities", *Journal of money laundering control,* vol. 20, pp. 1-7, 2017.

[8] Ken Naganuma, Masayuki Yoshino, Hisayoshi Sato, Takayuki Suzuki , " Auditable Zerocoin", *IEEE,* pp. 59-63, 2017.

[9] Krishna Priya.G, Dr.M.Prabaharan, "Money laundering analysis based on time variant behavioral transaction patterns using data mining", *Journal of Theoretical and applied information Technology,* vol. 67, pp. 12-17, 2014.

[10] 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.

[11] Malte Moser, Rainer Bohme, Dominic Breuker, "An Inquiry into Money Laundering Tools in the Bitcoin Ecosystem", *IEEE,* 2013.

[12] Murad Mehmet, Duminda wijesekera, "Using Dynamic Risk Estimation and Social Network Analysis to Detect Money Laundering Evolution", *IEEE,* pp. 310-315, 2013.

[13] Nhien An Le Khac, Sammer Markos, M.Teharkechadi, "A Data Mining Based Solution For Detecting Suspicious Money Laundering Cases in an Investment Bank", Second International Conference on Advances in Databases, Knowledge, Data Applications, *IEEE,* 2010, pp. 235-240.

[14] Pankaj Richhariya, Prahankk Singh, Endu Duneja, "A Survey on Financial Fraud Detection Methodologies", *International Journal of Commerce Business and Management,* vol. 45, pp. 15-22, 2012.
[15] Saeideh Alimolaei, "An Intelligent system for User Behavior detection in Internet Banking", 4th Iranian Joint Congress on Fuzzy and Intelligent Systems (CFIS), *IEEE*, 2015, pp. 1-5.
[16] Vikas Jayasree, R.V.Siva Balan, "Money Laundering Regulatory Risk Evaluation Using Bitmap Index-Based Decision Tree", *Journal of the Association of Arab Universities for Basic and Applied Sciences,* vol. 23, pp. 96-102, 2017.
[17] Xingrong Luo, "Suspicious transaction detection for Anti Money Laundering", *International Journal of Security and Its Applications,* vol. 8, pp. 157-166, 2014.

AUTHORS

A. Helen – A. Helen is currently pursuing her M.E Degree in Computer Science and Engineering from Easwari Engineering College, Chennai, Tamilnadu, India. She received her B.E Degree from Anna University, Chennai in the year 2015. Her Areas of Interest Includes Web Mining, Data Warehousing, and Mining. Email- helencanute@gmail.com

S. Sobitha Ahila – S. Sobitha Ahila Ph.D. works as Associate Professor in Easwari Engineering College, Chennai, TamilNadu, India. She received her B.E. Degree from Madurai Kamaraj University in the year 1997, M.E. Degree from Bharathidhasan University, Trichy in the year 2002 and a Ph.D. degree from Anna University, Chennai in the year October 2016. She has more than 14 years teaching experience and her areas of specializations are Data Analytics, Web mining, Multi-Agent systems.
Email- sobitha.ooviya@gmail.com

A. Niranjana – A. Niranjana B.Tech., M.E., works as Assistant Professor in Easwari Engineering College, Chennai, TamilNadu, India. She received her B.Tech. Degree from Anna University in the year 2010, M.E. Degree from Anna University, Chennai in the year 2012. She has more than 5 years teaching experience and her areas of specializations are Wireless Sensor Networks and Biomedical Engineering.
Email- nithu6289@gmail.com

