Survey of Common Design Approaches in AML Software Development

Alexander Semenov
JSC NICEVT
Moscow, Russia
alxdr.semenov@gmail.com

Artem Mazeev
JSC NICEVT
Moscow Institute of Physics and Technology
Moscow, Russia
mav367@mail.ru

Dmitry Doropheev
Moscow Institute of Physics and Technology
Moscow, Russia
dmitry@dorofeev.su

Timur Yusubaliev
Quality Software Solutions ltd
Moscow, Russia
ytr@kpr-it.com

Abstract

In the recent years, money laundering activity has become more and more ubiquitious all over the world. In the paper we survey the technical aspects of anti-money laundering systems (AML). We briefly present the principles of money laundering process and features of the illegal activity that can arise in the graph of money transactions, company or user profiles. Then we present a detailed analysis of anomaly detection, machine learning and neural networks techniques in the context of AML systems.

Keywords: anti-money laundering, machine learning, anomaly detection, graph mining

1 Introduction

Money laundering (ML) is a criminal activity or process that deals with criminal proceeds to disguise their illegal origin and make them appear legitimate. In recent years, money laundering activity is becoming more and more ubiquitious all over the world [1]. Between 1.5 trillion USD and 2.8 trillion USD or between 2% and 5% of global gross domestic product (GDP) is lost annually through money laundering worldwide [2].

In: V. Voevodin, A. Simonov (eds.): Proceedings of the GraphHPC-2017 Conference, Moscow State University, Russia, 02-03-2017, published at http://ceur-ws.org.

The role of financial institutions is to find ways to identify, among the huge number of operations that occur every day, those suspicious transactions and then investigate them in more detail [3]. There are many illegal money laundering schemes of complex nature, and new sophisticated schemes appear exploiting ever increasing richness of money forms and economic activity [4]. Some schemes are recognized by FATF (Financial Action Task Force inter-governmental organization that aims to set standards and promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system [5]).

There are a large number of papers that consider the solution of this problem, but most of them belong to authors from China [6], Australia, India [7], Sweden, [8], Poland, Ireland [9], Egypt [10], Pakistan [11], Saudia. IT Giants and authors from the most advanced natures do not publish papers which contain technical considerations of anti-money laundering (AML) systems with corresponding keywords.

There exist only small number of survey articles on AML systems and algorithms [12, 13, 14]. Related works are cited in [11,15,16,17] and some other papers.

Besides money laundering there is another type of illegal activity. Fraud is a crime where the objective is to gain money by an illegal form [18]. Fraud detection is similar to money laundering but our survey considers only money laundering.

The survey is an introduction to technical and corresponding aspects of anti-money laundering systems.

The organization of the survey is as follows. Section 2 deals with principles of money laundering process and features of the illegal activity that can be found in the graph of money transactions, company or user profiles. Section 3 provides a historical review of main anti-money laundering approaches. Section 4 presents detailed analysis of the state-of-the-art techniques and AML systems. Finally, we conclude in Section 5 .

2 Money Laundering Features

The process of money laundering usually consists of three stages [19]:

- **Placement** is a transfer of cash into financial system. Placement is carried out in credit institutions, security markets, retail trading. The goal of placement is to conceal or disguise source or ownership of the illegal funds. Often funds are placed in the foreign countries. The stage of placement of criminal proceeds is the most unreliable stage in the process of money laundering. At this stage there is the best chance to identify illegally received funds.
- **Layering** is a separation of criminal proceeds from their sources through complex chains of financial transactions aimed at disguising the trace of the illegal funds. Various financial operations overlap one another in order to complicate the work of AML systems and experts aimed to identifying criminal proceeds and persons who legalize them. If the placement of criminal funds was successful, that is, it was not discovered, then it becomes much more difficult to detect illegal operations at this stage.
- **Integration** is the last stage of the legalization process, directly aimed at creating the appearance of legality to the criminally obtained capital. Funds separated in the previous stages are consolidated at the integration stage into some form, which is convenient for the customer: money on the account in a first-class bank, liquid securities, real property assets. The laundered funds are invested further in the legal sectors of the economy, which also creates a basis for new crimes. To simplify further legalization of funds, criminal communities acquire credit organizations and other financial institutions, and also buy significant shares in the ownership of enterprises in the real sector of the economy, transferring them under their own control. If the money laundering trace has not been identified in the two previous stages, then it is extremely difficult to separate legal funds from illegal ones at the integration stage.

However, there are also two-stage and four-stage models [20]. In the four-stage model placement occurs simultaneously in many places (small amounts for many different accounts, often through acquaintances, relatives).

The financing of terrorism differs from money laundering in that the funding sources can be of legal origin.

It is clear from the three-stage model that a typical money laundering scheme involves multiple transactions, conducted through a variety of different channels, banks, by a group of parties (individuals, businesses, etc.).

Different schemes can be borrowed from the rules of committees that exist in different states. For example, in USA [21], in Australia [22]. There are also state-controlled organizations that help businesses, for example in the USA — FINRA [23]. Some typical money laundering schemes are described in [19, 24].

Basic characteristics of a money laundering scheme are the following: a role assignment between the parties, a particular execution order of the transactions, synchronization of transactions as per time and the amount of transactions, etc.

The authors of [25] note the following important features for AML:

- Type of the main activity of the company (retail, gambling, intermediary services);
- Type, amount and size of transactions (cash receipt, withdrawal of cash from ATM);
- Geographical factor (offshore operation, participation in the transaction of the company or a bank with a critically low level of AML);
- Specificity of the organizational structure (for example, the company with too young founders);
- Events preceding the transaction (changes in the ownership of the company, obtaining a large loan);
- Transaction history.

2.1 Client Profiling

In AML it is important to determine potential risky parties (users, clients). AML systems can have an increased focus on risky users.

The following can be used as features of risky users [3, 26]:

- Large deposits and withdrawals;
- Periodicity of transactions;
- Transactions in risky areas regarding money laundering (in free trade-industrial zones);
- Transactions of less than a specified threshold amount in order to avoid control of AML systems;
- Degree of bank service usage;
- Reactivation of off-line accounts;
- Account age.

2.2 Graph Patterns

Money laundering can be detected in the graph of money transactions. Relations between parties in the graph of money transactions produce social network. The graph mining methods and methods of social networks analysis can be applied to detect suspicious transactions [27].

There are different patterns (templates) in the transaction graph that can be suspicious. A common structure of a subgraph is in Figure 1 and can correspond to the placement, layering and integration model. Initially money is placed in X vertex. Two other typical AML subgraphs are shown in Figures 2 and 3. It refers to cyclic business activity to conceal money's genesis. Of course, these examples are only schematic and real subgraphs can be different and complicated. Many relevant papers solve the problem of searching of clusters in the graph by some criteria.

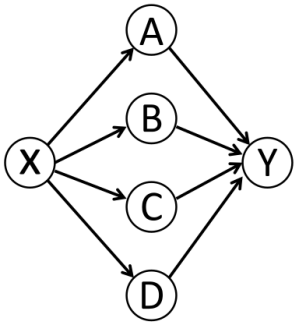

Figure 1: Common structure of a subgraph in the placement, layering and integration model.

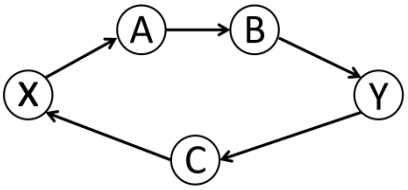

Figure 2: Common structure of a subgraph representing illegal cyclic business activity.

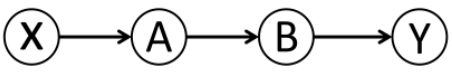

Figure 3: AML subgraph pattern.

Real graph patterns can be highly complicated. In the paper [28] an algorithm for searching of "volcanoes" and "black holes" patterns is proposed, which actually represents the placement, layering and integration model. Figure 4 shows these patterns.

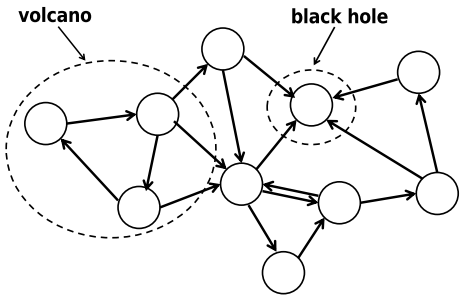

Figure 4: "Volcanoes" and "black holes" in the transaction graph.

3 Anti-Money Laundering Principles

The AML problem can be solved by using different approaches:

- Rule-based approach;
- Anomaly detection;
- Machine learning.

One of the first AML-systems [29] was created in 1995 and was based on **rules**. Rules can be very complex and can be defined with use of decision trees [30]. Rules are formulated by experts and can very accurately detect criminal schemes. However, this technique is human dependent, not flexible and not automatic. Further, it can not be used to recognize new typologies of fraudulent transactions.

Data mining techniques involve interdisciplinary methods from machine learning, statistics and databases. **Anomaly detection** [31, 32, 33] is the one of the data mining problems. Systems that use the anomaly detection began to appear after systems based on rules. The report [34] provides an overview of data mining techniques for detecting fraud in different areas. The advantages of anomaly detection are a capability of discovering new laundering patterns and an ability to customize normal activities.

Machine learning and **artificial intelligence** are big topics in the financial services sector these days. Machine learning is increasingly used in the modern systems [15, 35]. The most popular problem is the classification problem (two-class classification). The goal is to define whether the given transaction is suspicious or not after procedure of training on precedents. The test set of precedents specifies information, which transactions are suspicious and which are not.

The problem can be considered in terms of probability, when for each transaction a probability (weight) of transaction being suspicious is assigned. The Bayesian classification methods can be used for the problem.

This type of detection is only able to detect frauds similar to those which have occurred previously and have been classified by a human. To detect a novel type of fraud it may require the use of an unsupervised machine learning algorithm.

Earlier AML-systems often used the principle of analyzing the actions of a particular person, but in modern AML-systems, the analysis of the network (or graph) of transactions is increasingly used. For example, in [36] on the basis of bank data, a social network is built between the clients of the bank, which are connected by transactions.

The papers [25, 37] consider a search of patterns in graphs (template subgraphs) that are most similar to the known patterns. The principle of approximate search is applied when there is no need for a fixed pattern matching, which means that the search is more flexible as it allows some deviation from the templates.

4 Modern Techniques and Systems

It is hard to strictly classify approaches to the development of AML systems. Each AML subsystem can uses different data mining techniques.

4.1 Anomaly Detection

Anomaly detection is an identification of elements of a given dataset that do not conform to the expected pattern. These anomalies occur very infrequently but may signify a large and significant threat such as cyber intrusions or fraud, i.e. it is necessary to detect the anomaly (suspicious) data in the background of the other data.

The advantages of anomaly detection are capability of discovering new laundering patterns and customization ability of normal activities. The anomaly detection drawback is a high rate of false alarms.

The **unsupervised** anomaly detection techniques do not need training data. This kind of methods is beneficial when some abnormal behavior has not been demonstrated in the training sample, for example, if the sample is small.

There are a large number of methods and algorithms for anomaly detection [32], for example: clustering techniques [38], unsupervised neural network, fuzzy C-means [39].

A set of the features is necessary for algorithms of anomaly detection as well as for supervised learning. Note that the vector of features (numbers) can be represented as a point in n-dimensional space (where n is the number of features). The goal of the algorithm is to find unusual points (outliers). Outliers can be searched using different algorithms [40], for example, using the K-nearest neighbors algorithm [41].

It is also possible to use statistical methods to anomaly detection [31]. One needs to build distribution function of some feature as a random variable, and then select the parameters, by which the outliers can be detected.

Despite the absence of the training phase, it is possible to develop some method of determining the suspicious transactions to suggest the user, which transactions may be suspicious. For example, a good simple idea is to use the knowledge about customers and detect activities that are not typical for reliable clients [42].

The clustering based techniques group customers that perform similar kind of transactions into a single cluster and then categorize either small-size clusters or outliers as anomalous [11].

Theoretically, **supervised** anomaly detection methods can provide better results than unsupervised methods, since they are based on more information. However, the training sets usually contain some noises that result in higher false alarm rates, and obtaining accurate training set is a difficult problem [33].

4.2 Graph Mining

Many techniques have been developed in the past decades for spotting outliers and anomalies in unstructured collections of multi-dimensional data points. On the other hand, data objects cannot always be treated as points lying in a multi-dimensional space independently [43]. Transaction graph is a good abstraction for data represeting in AML systems, inter-dependencies between transactions should be accounted for during the anomaly detection process. In [43] a comprehensive survey of **graph based anomaly detection** techniques is presented.

Graph pattern matching or graph isomorphism can be appropriate technique for searching abnormal subgraphs in the transaction graph. But exact matching makes too strict requirements, and inexact algorithms should be used instead. For example, in the paper [28] an algorithm for searching of “volcanoes” and “black holes” patterns is proposed, which actually represent the placement, layering and integration model. Figure 4 shows these patterns.

Database information about attendees and their relations can be useful for anti-money laundering algorithms. So social network analysis can be additional technique that can be used in AML systems [44]. For example, in [36] on the basis of bank data, a social network is built between the clients of the bank, which are connected by transactions. Features are calculated

for each customer (betweenness centrality, page rank, etc.). Based on the features, each client is assigned a role, for example, it can be an isolator role that isolates a certain group of clients from the rest; Another role – the role of a communicator, which, on the contrary, connects several groups of customers. Further analysis of new transactions checks whether the previously identified role of the client is consistent with its new behavior.

4.3 Fuzzy Graph Patterns

In modern AML systems, the search of subgraphs that approximately satisfy the given criteria is an important component. The problem is called fuzzy graph isomorphism. In [25] authors present an algorithm for finding a fuzzy set of maximal cliques, they claim that method based on the algorithm can contribute to modern AML systems that use comprehensive information from various information sources about actors as well as experts evaluation.

In [37] authors propose a method for mining transcation graphs based on building a model that is parametrized by fuzzy numbers. These numbers represent parameters of transactions and of the transaction subgraphs to be detected. The method uses genetic algorithm for parameters optimization.

4.4 Client Profiling Systems

It has been noted that in AML systems it is important to determine potential risky parties (users, clients).

In [3] a client profiling subsystem is proposed. All bank clients are clusterized with use of k-means [45] and other algorithms by some features. Unsupervised anomaly detection techniques are used for discovering new patterns with subsequent rule generation algorithm [46].

In [26] fuzzy rules are used for description generation of risky users. Fuzzy rules retain the advantages of fuzzy expert systems, while reducing the need for an expert. The 5-layered neural network trains and improves the fuzzy rules. The training method includes a combination of least squares and back propagation.

4.5 Machine Learning

In recent years, machine learning and artificial intelligence have seen an increasing interest and popularity in the financial services community [15, 37, 47, 48]. Machine learning is a particularly powerful tool for prediction purposes. Supervised methods (also known as classification methods) required a labeled training set containing both normal and anomalous samples to construct the predictive model.

AML system based on machine learning principles is described in the next subsection 4.5.1 .

4.5.1 Australian AML system

The Australian AML system developed for the Australian Transaction Reports and Analysis Centre (AUSTRAC) [49] is described in the recent papers [15, 50] in 2016, 2017.

The system analyzes two types of transactions: large cash deposits and oversea transfers. The subject of the analysis is a graph in which parties are connected by edges of two types: one type for transaction, another type for suspicious relations between parties. There can be a lot of suspicious relation cases, for example, two persons own the same account. Transaction edge has a weight.

The system performs the following actions:

1. Modeling of relationships between parties using a graph with attributes;
2. Community extraction from the transaction graph;
3. Calculation of the features from the extracted communities;
4. Supervised learning.

Fig. 5 shows the general scheme of the system.

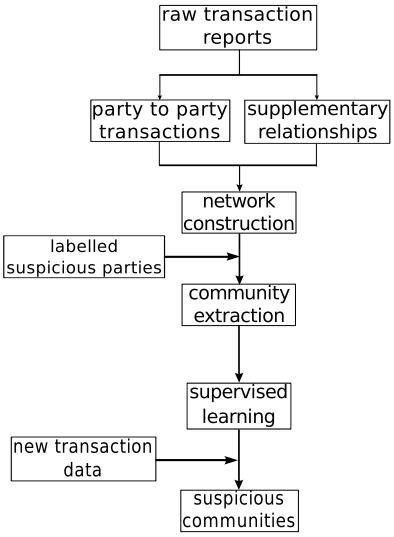

Figure 5: Scheme of the Australian AML system.

The development of algorithms for community detection in a graph with attributes is an important scientific challenge. There are only limited number of concerned papers, for example, the preprint of the paper [51]. The existing community detection algorithms can be poorly adapted to a specific task, for example, they detect communities of too large size. At the same

time, in the problem of detection of suspicious transactions the size of the criminal communities are relatively small.

The k-step neighbors algorithm is used to community extraction in the considered system. Authors use its own methodology for processing the communities that can overlap.

Algorithms of the classification problem in machine learning need a set of formalized features of each object. In the considered system different features are calculated for the extracted communities. Features are determined by experts (unpublished, closed part of the paper). Authors note that features can be divided into several categories:

1. Demography. Aggregated features that describe persons in the graph, for example, the average age;
2. Graph. Features that describe the structure of the graph;
3. Transaction. Aggregated features that describe transactions in the extracted communities, for example, total sum of transactions;
4. Dynamics. Varied over time features. For example, the number of rapidly changing transaction sizes.

In the system a support vector machine (SVM) and a random forest is used as machine learning algorithms. Evaluation of the system gains 74–98 % precision, the authors claim that the constructed classifiers are able to achieve a level of performance that is suitable for use in a real environment.

4.6 Neural Networks

It seems that while machine learning techniques are sufficient for AML purposes, neural networks seems to be too powerful tool for AML. But there are several examples of using neural networks in AML.

In [1] authors propose a radial basis function (RBF) neural network model based on clustering algorithm. An RBF network is a three-layer feed-forward neural network which consists of an input layer, a hidden layer, and an output layer. RBF network uses center vectors as the parameters of the hidden layer. In the proposed algorithm center vectors are obtained by clustering algorithm. During the training stage the algorithm clusters the sample data, the centers of clusters are center vectors of radial basis function. The authors note that SVM can get good result, but the time cost is high. The proposed method is compared against support vector machine (SVM) and outlier detection methods, which show that the proposed method has the highest detection rate and the lowest false positive rate.

In [26] a 5-layered neural network trains and improves the fuzzy rules, which are used for generation of risky users description. The training method includes a combination of least squares and back propagation.

5 Conclusion

In the paper we survey the technical aspects of anti-money laundering systems. We briefly present the principles of money laundering process and features of illegal activity that can arise in the graph of money transactions, company or user profiles. Then we present a detailed analysis of anomaly detection, machine learning and neural networks techniques, and the modern Australian AML system.

Research is being conducted with the finance support of the Ministry of Education and Science of the Russian Federation Unique ID for Applied Scientific Research (project) RFMEFI57816X0218. The data presented, the statements made, and the views expressed are solely the responsibility of the authors.

References

[1] Y. Yang, B. Lian, L. Li, and P. Li, "A RBF neural network model for anti-money laundering," *Proceedings of the Wavelet Analysis and Pattern Recognition International Conference*, pp. 209–215, 2008.

[2] B. Unger, "Offshore Activities and Money Laundering: Recent Findings and Challenges," *European Parliament Directorate-General for Internal Policies*, 2017. `http://www.europarl.europa.eu/RegData/etudes/STUD/2017/595371/IPOL_STU(2017)595371_EN.pdf` (accessed: 29.09.2017).

[3] C. Alexandre and J. Balsa, "Client Profiling for an Anti-Money Laundering System," *CoRR*, vol. abs/1510.00878, 2015. `https://arxiv.org/pdf/1510.00878.pdf` (accessed: 29.09.2017).

[4] C. Jedrzejek, M. Falkowski, and J. Bak, "Graph Mining for Detection of a Large Class of Financial Crimes," `http://ceur-ws.org/Vol-483/paper4.pdf` (accessed: 29.09.2017).

[5] *Financial Action Task Force (FATF).* `http://www.fatf-gafi.org/home/` (accessed: 29.09.2017).

[6] X. Luo, "Suspicious Transaction Detection for Anti-Money Laundering," *International Journal of Security and Its Applications*, vol. 8,

no. 2, pp. 157–166, 2014. http://www.sersc.org/journals/IJSIA/vol8_no2_2014/16.pdf (accessed: 29.09.2017).

[7] C. Suresh, K. T. Reddy, and N. Sweta, "A Hybrid Approach for Detecting Suspicious Accounts in Money Laundering Using Data Mining Techniques," *Information Technology and Computer Science*, pp. 37–43, 2016.

[8] E. A. Lopez-Rojas and S. Axelsson, "Multi Agent Based Simulation (MABS) of Financial Transactions for Anti Money Laundering (AML)," pp. 25–32, 10 2012. http://www.diva-portal.org/smash/get/diva2:834702/FULLTEXT01.pdf (accessed: 29.09.2017).

[9] N. LeKhac and M.-T. Kechadi, "Toward a new cloud-based approach to preserve the privacy for detecting suspicious cases of money laundering in an investment bank," *International Conference on Computational Science*, 2014. http://researchrepository.ucd.ie/bitstream/handle/10197/6553/insight_publication.pdf?sequence=1 (accessed: 29.09.2017).

[10] A. K. A. A. El-Din and N. E. Khamesy, "Data Mining Techniques for Anti Money Laundering," *International Journal of Advanced Research in Science, Engineering and Technology*, vol. 146, 2016.

[11] A. S. Larik and S. Haider, "Clustering based anomalous transaction reporting," *Procedia Computer Science*, vol. 3, pp. 606 – 610, 2011. http://www.sciencedirect.com/science/article/pii/S187705091000476X (accessed: 29.09.2017).

[12] K. D. Rohit and D. B. Patel, "Review On Detection of Suspicious Transaction In Anti-Money Laundering Using Data Mining Framework," *International Journal for Innovative Research in Science & Technology*, vol. 1, 2015. http://www.ijirst.org/articles/IJIRSTV1I8043.pdf (accessed: 29.09.2017).

[13] K. Manjunath, "Data Mining Techniques for Anti Money Laundering," *International Journal of Advanced Research in Science Engineering and Technology*, vol. 2, 2015. http://www.ijarset.com/upload/2015/august/1_IJARSET_manjunath.pdf (accessed: 29.09.2017).

[14] N. A. L. Khac, S. Markos, M. O'Neill, A. Brabazon, and M.-T. Kechadi, "An investigation into Data Mining approaches for Anti Money Laundering," *International Conference on Computer Engineering and Applications*, vol. 2, 2009. http://www.ipcsit.com/vol2/94-C140.pdf (accessed: 29.09.2017).

[15] D. Savage, Q. Wang, X. Zhang, P. Chou, and X. Yu, "Detection of Money Laundering Groups: Supervised Learning on Small Networks," 2017. https://aaai.org/ocs/index.php/WS/AAAIW17/paper/view/15101 (accessed: 29.09.2017).

[16] N.-A. Le-Khac, S. Markos, and M.-T. Kechadi, "A Heuristics Approach for Fast Detecting Suspicious Money Laundering Cases in an Investment Bank," *International Journal of Computer, Electrical, Automation, Control and Information Engineering*, vol. 3, no. 12, 2009. http://waset.org/publications/12189/a-heuristics-approach-for-fast-detecting-suspicious-money-laundering-cases-in-an-investment-bank (accessed: 29.09.2017).

[17] N. A. L. Khac, S. Markos, and M.-T. Kechadi, "A Data Mining-Based Solution for Detecting Suspicious Money Laundering Cases in an Investment Bank," pp. 235–240, 2010.

[18] M. P. S.-B. Almeida, "Classification for fraud detection with social network analysis," *Masters Degree Dissertation, Engenharia Informatica e de Computadores*, 2009.

[19] A. Samantha Maitland Irwin, K.-K. Raymond Choo, and L. Liu, "An analysis of money laundering and terrorism financing typologies," *Journal of Money Laundering Control*, vol. 15, no. 1, pp. 85–111, 2011. http://search.ror.unisa.edu.au/media/researcharchive/open/9915914120301831/53109886220001831 (accessed: 29.09.2017).

[20] I. Kozlov, "About the stages of the money laundering process," *Finance and credit*, vol. 31, no. 278, pp. 76–79, 2007.

[21] *Guide to U.S. Anti-Money Laundering Requirements.* https://www.protiviti.com/sites/default/files/united_states/insights/guide-to-us-aml-requirements-6thedition-protiviti_0.pdf (accessed: 29.09.2017).

[22] *Australian Registered AML/CTF Rules.* http://www.austrac.gov.au/businesses/

legislation/registered-amlctf-rules (accessed: 29.09.2017).

[23] *Financial Industry Regulatory Authority.* http://www.finra.org/industry/aml (accessed: 29.09.2017).

[24] A. S. M. Irwin, K.-K. R. Choo, and L. Liu, "Modelling of Money Laundering and Terrorism Financing Typologies," *Journal of Money Laundering Control*, vol. 15, no. 3, pp. 316–335, 2012. https://www.researchgate.net/publication/263332155_Modelling_of_Money_Laundering_and_Terrorism_Financing_Typologies (accessed: 29.09.2017).

[25] L. S. Bershtein and A. A. Tselykh, "A Clique-based Method for Mining Fuzzy Graph Patterns in Anti-money Laundering Systems," pp. 384–387, 2013. http://doi.acm.org/10.1145/2523514.2523568 (accessed: 29.09.2017).

[26] N. Heidarinia, A. Harounabadi, and M. Sadeghzadeh, "An Intelligent Anti-Money Laundering Method for Detecting Risky Users in the Banking Systems," *International Journal of Computer Applications*, vol. 97, no. 22, 2014. http://research.ijcaonline.org/volume97/number22/pxc3897780.pdf (accessed: 29.09.2017).

[27] R. Drezewski, J. Sepielak, and W. Filipkowski, "The Application of Social Network Analysis Algorithms in a System Supporting Money Laundering Detection," *Inf. Sci.*, vol. 295, no. C, pp. 18–32, 2015. https://www.researchgate.net/publication/267632670_The_application_of_social_network_analysis_algorithms_in_a_system_supporting_money_laundering_detection (accessed: 29.09.2017).

[28] Z. Li, H. Xiong, and Y. Liu, "Detecting Blackholes and Volcanoes in Directed Networks," *CoRR*, 2010. https://arxiv.org/pdf/1005.2179.pdf (accessed: 29.09.2017).

[29] T. E. Senator, H. G. Goldberg, and J. W. et al., "Financial Crimes Enforcement Network AI System (FAIS) Identifying Potential Money Laundering from Reports of Large Cash Transactions," *AI Magazine*, vol. 16, no. 4, pp. 580–585, 1995.

[30] S.-N. Wang and J.-G. Yang, "A Money Laundering Risk Evaluation Method Based on Decision Tree," *Machine Learning and Cybernetics, 2007 International Conference on*, 2007. https://pdfs.semanticscholar.org/5c31/e690df172d631b933dd60a81a168f928d02d.pdf (accessed: 29.09.2017).

[31] C. Wang, K. Viswanathan, L. Choudur, V. Talwar, W. Satterfield, and K. Schwan, "Statistical Techniques for Online Anomaly Detection in Data Centers," *IFIP/IEEE International Symposium on Integrated Network Management*, 2011. http://www.hpl.hp.com/techreports/2011/HPL-2011-8.pdf (accessed: 29.09.2017).

[32] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly Detection: A Survey," *ACM Computing Surveys*, vol. 41, no. 15, 2009. http://cucis.ece.northwestern.edu/projects/DMS/publications/AnomalyDetection.pdf (accessed: 29.09.2017).

[33] S. Omar, A. Ngadi, and H. H. Jebur, "Machine Learning Techniques for Anomaly Detection: An Overview," *International Journal of Computer Applications*, vol. 79, no. 2, pp. 33–41, 2013. http://research.ijcaonline.org/volume79/number2/pxc3891478.pdf (accessed: 29.09.2017).

[34] C. Phua, V. Leea, K. Smith, and R. Gayler, "A Comprehensive Survey of Data Mining-Based Fraud Detection Research," 2010. https://www.google.ru/url?sa=t&rct=j&q=&esrc=s&source=web&cd=10&ved=0ahUKEwihoJ-ijYHRAhUDiiwKHZyGBHAQFghbMAk&url=https%3A%2F%2Fsites.google.com%2Fsite%2Fcliftonphua%2Ffraud-detection-survey.pdf&usg=AFQjCNEWy-HRGI-yrgXlOcY5lOkDmn9V5w&sig2=5bIw1d1Z5wtoyn_XCNAykA&cad=rjt (accessed: 29.09.2017).

[35] A. D. Pozzolo, O. Caelen, Y.-A. L. Borgne, S. Waterschoot, and G. Bontempi, "Learned lessons in credit card fraud detection from a practitioner perspective," *Expert Systems with Applications*, vol. 41, pp. 4915–4928, 2014.

[36] R. Drezewski, G. Dziuban, ukasz Hernik, and M. Paczek, "Comparison of Data Mining Techniques for Money Laundering Detection System," *Conference: 2015 International Conference on Science in Information Technology*, 2015.

[37] K. Michalak and J. Korczak, "Graph Mining Approach to Suspicious Transaction Detection," *Proceedings of the Federated Conference on Computer Science and Information Systems*, 2011. https://fedcsis.org/proceedings/2011/pliks/218.pdf (accessed: 29.09.2017).

[38] P. Berkhin, "Survey of Clustering Data Mining Techniques," http://www.cc.gatech.edu/~isbell/reading/papers/berkhin02survey.pdf (accessed: 29.09.2017).

[39] R. Winkler, F. Klawonn, and R. Kruse, "Problems of Fuzzy c-Means Clustering and Similar Algorithms with High Dimensional Data Sets," 2010.

[40] P. Kanhere and H. K. Khanuja, "A Survey on Outlier Detection in Financial Transactions," *International Journal of Computer Applications*, vol. 108, no. 17, 2014. http://research.ijcaonline.org/volume108/number17/pxc3900502.pdf (accessed: 29.09.2017).

[41] J. M. Keller, M. R. Gray, and J. James A. Givens, "A Fuzzy K-Nearest Neighbor Algorithm," *IEEE Transactions on Systems, Man, and Cybernetics*, vol. SMC-15, no. 4, pp. 580–585, 1985. https://myteks.files.wordpress.com/2012/03/fuzzyknn.pdf (accessed: 29.09.2017).

[42] J. Kingdon, "AI Fights Money Laundering," *IEEE Intelligent Systems*, vol. 19, pp. 87–89, may 2004. https://pdfs.semanticscholar.org/0380/c04339f606413c71b657fab8ee3e4556c046.pdf (accessed: 29.09.2017).

[43] L. Akoglu, H. Tong, and D. Koutra, "Graph Based Anomaly Detection and Description: A Survey," *Data Min. Knowl. Discov.*, vol. 29, pp. 626–688, May 2015. https://arxiv.org/pdf/1404.4679.pdf (accessed: 29.09.2017).

[44] M. Pironet, C. Antunes, P. Moura, and J. Gomes, "Classification for Fraud Detection with Social Network," https://fenix.tecnico.ulisboa.pt/downloadFile/395138965337/ResumoAlargadoFinalEntregue.pdf (accessed: 29.09.2017).

[45] G. Hamerly and C. Elkan, "Alternatives to the K-means Algorithm That Find Better Clusterings," pp. 600–607, 2002. http://people.csail.mit.edu/tieu/notebook/kmeans/15_p600-hamerly.pdf (accessed: 29.09.2017).

[46] E. Frank and I. H. Witten, "Generating Accurate Rule Sets Without Global Optimization," pp. 144–151, 1998. https://pdfs.semanticscholar.org/3998/12d46345ad7d93f5510b1bbda30948e7a65c.pdf (accessed: 29.09.2017).

[47] B. van Liebergen, "Machine Learning: A Revolution in Risk Management and Compliance?," *The Capco Institute Journal of Financial Transformation*, vol. 4, 2017. https://www.iif.com/system/files/32370132_van_liebergen_-_machine_learning_in_compliance_risk_management.pdf (accessed: 29.09.2017).

[48] E. A. Lopez-Rojas and S. Axelsson, "Money Laundering Detection using Synthetic Data," *The 27th annual workshop of the Swedish Artificial Intelligence Society (SAIS)*, 2012. http://www.ep.liu.se/ecp/071/005/ecp12071005.pdf (accessed: 29.09.2017).

[49] *Australian Transaction Reports and Analysis Centre*. http://www.austrac.gov.au (accessed: 29.09.2017).

[50] D. Savage, Q. Wang, P. Chou, X. Zhang, and X. Yu, "Detection of money laundering groups using supervised learning in networks," 2016. https://arxiv.org/pdf/1608.00708.pdf (accessed: 29.09.2017).

[51] J. Yang, J. McAuley, and J. Leskovec, "Community Detection in Networks with Node Attributes," 2014. https://arxiv.org/pdf/1401.7267v1.pdf (accessed: 29.09.2017).