International Journal of Latest Research in Science and Technology **ISSN (Online):2278-5299**
Volume 7, Issue 3: Page No.1-9 ,May-June 2018
https://www.mnkpublication.com/journal/ijlrst/index.php

EXPERT SYSTEM FOR THE DETECTION OF SUSPICIOUS BANKING TRANSACTIONS OF MONEY LAUNDERING

Juan Francisco Sabas González[1*] ,Tonáhtiu Arturo Ramírez Romero[2],Miguel Patiño Ortiz[3]
[1,2,3]*SEPI, ESIME, IPN Instituto Politécnico Nacional SEPI, ESIME, IPN*
[1]jfcosabas@gmail.com, [2]tonahtiu@yahoo.com, [3]mpatino2002@gmail.com
México

Abstract- **Money laundering (ML) is one of the main issues today, because it has a great impact on the economy and society of the countries. This crime is carried out by criminal organizations that need to hide the origin of illicit money obtained from their activities, and this is achieved by disguising illicit money transactions through banks. In Mexico, in the year 2015 ten thousand millions of dollars were washed, for this reason an expert system was created, in this paper presents how the structure of the proposed expert system works, and that its main function is the evaluation of clients' transactions by an algorithm with a decision tree approach and based on rules to identify if their transactions are suspicious.**

Keywords **–** detection, expert system, money laundering, suspicious transactions.

I. INTRODUCTION

Money laundering is a form of concealment of illicit money obtained from various crimes such as drug trafficking, terrorism, human trafficking, animal trafficking, etc. The process to carry out money laundering is through a cycle which has three phases:

1. Placement: introduction of resources of illicit origin to the economy.
2. Stratification: perform operations to hide their origin and prevent trace of the source.
3. Integration: insertion of illegal funds into the economy as legitimate funds.

This cycle makes the illicit money become legitimate and cannot be traced from where it came.

In 2015, The Intelligence Unit of Mexico, reported that in 2014 there were eighty-seven complaints of money laundering. This represents an increase of 65% with respect to 2006 [1]. On the other hand, the Basel Institute locates Mexico as one of medium-risk countries to carry out money laundering [2].

Therefore, multiple banking in Mexico is fighting a big problem that is money launderingwith the passage of time, some expert systems have been developed, and several conventional techniques and computational technologies have been used to detect suspicious transactions.

II. RELATED WORKS

Patcha[3] mentions some of them, but the techniques and methods for detection, as seen below:

Rational Choice Theory

Nicholas Gilmour [4]created a theory composed of five stages that covers the collection of data, analysis, study of opportunities for prevention, application of feasible and economic measures.

This theory serves to understand the environment surrounding the money laundering process, given the assumption of rational decisions taken by organized crime in money laundering measures

Decision Trees

Inwang and Yang [5] propose a method that evaluates the transactions made by client to determine if they are suspicious of money laundering, this method uses a decision tree structure based on the ID3 [6] algorithm, and on the other hand it uses rules that help the inferences.

VikasJayasree and R.V. Siva Balan [7] assess the risk that a financial organization is committing the illicit act of money laundering, through the use of decision trees built with a bitmap index.

Rule Based Systems

RafalDrezewski, Jan Sepielak and WojciechFilipkowski[8], created a rule-based money laundering detection system, which imports customer account statements into the CAST / LINK system module, which is composed of 6 stages:

1. Bank statement import module.
2. Clustering module.
3. Suspected sequences / sets of cluster module.

Publication History
Manuscript Received :
Manuscript Accepted :
Revision Received :
Manuscript Published :

4. Company / organization profile generation module.
5. Social media analysis module.
6. Data visualization and interaction with the user module.

Intelligent Agents

ShijiaGao[9]created a money laundering prevention system with decision support through 5 Intelligent agents:

1. User agent
2. Data collector agent
3. Monitoring agents
4. Behavioral diagnostic agent
5. Information agent

Which focus on the analysis, monitoring and diagnosis of suspicious transactions made by customers.

Clustering

Xingqi Wang, Guang Dong[10] developed an algorithm to detect suspicious operations of money laundering, which uses improved minimum expansion tree clustering. This algorithm groups operations through a metric of similarity and dissimilarity between points in the data space.

AsmaLarik and SajjadHaider [11] use the Theory of Euclidean Adaptive Resonance Transformed in their system, which as a function to group clients in different clusters; and at the same time performs a calculation of the anomaly index based on the quantity and frequency to classify the transactions as anomalous

Bayesian

Raza y Haider [12] created a system for reporting suspicious activities, which consists of 3 stages: the first is to use the grouping technique, then dynamic Bayesian networks and finally an index to locate the probable anomalies in a sequence of operations.In a general way, it proposes to take periods of a user's transactions and obtain the patterns, these patterns perform a comparison process and any deviation from these patterns identifies them as suspicious.

Data Mining

Xingrong Luo [13] proposes a suspicious transaction detection model, which performs this activities:

1. Stores transactional data.
2. Performs a pre-processing job for data cleaning and transformation.
3. The related data is selected for the data mining engine, where an algorithm based on classification is applied to dynamically detect suspicious transactions on transactional data flows.
4. The discovered knowledge is stored in a knowledge base, which is used in the visualization of the recommendation systems.

Hong, Liang, Gao, and Li[14], propose an Adaptive Anti Money Laundering Resource Allocation Model (AAMLRAM) based on Semi-Markov Decision Process (SMDP), to allocate resources optimally in the anti-money laundering domain, to analyze a report of suspicious transactions sent by the Financial Institutions.

Neural Networks

Lin-Tao Lv, Na Ji, Jiu-Long Zhang [15] adopted a radial basis function, which receives the parameters of the APC-III clustering algorithm that is in a hidden layer, and also uses a least squares recursive algorithm to update the weights of the connections between the hidden layer and the output layer that is applied to the three-layer direct-feed neural network, to determine if the transaction is illegal or not.

Transaction Flow Analysis

The system developed by P. Umadevi and E.Divya[16] is based on two algorithms that are used to analyze the flow of money:

1. Clustering.
2. Mining of frequent patterns.

The system uses the two algorithms for the analysis process to detect the suspicious transaction.

Social Media Analysis

Drężewski, Sepielak, and Filipkowski[17]. They used network analysis techniques in a database of internal transactions of a factoring company, to classify and map the relational data and present predictive models based on network metrics to evaluate the risk profiles of the customers involved in the business.

Two Phase System

The architecture of Shafea, Hossam, Abd, Salah and Mohamed Shafea [18] consisted in monitoring and investigating financial transactions, it contains support modules:

1. Data collection module.
2. Analysis of links.
3. Risk score

These modules help to make decisions if it is an illicit act.

Digital Forensic Practices and Database Analysis

The model created by Flores, Angelopoulou and Self [19], has three phases:

1. Understanding of the case.
2. Analysis and evaluation of the case.
3. Case report.

In these phases, databases and forensic tools are used, emphasizing data mining and data storage techniques to help investigations related to money laundering and the "Know Your Customer" policies defined within an organization.

Neuro Fuzzy System

The method proposed by Neda Heidarinia, Ali Harounabadi and Mehdi Sadeghzadeh[20], is an adaptive neuro-diffuse inference system.

According to the authors, the input data is extracted from the bank's data sets and the fuzzy system is designed based on the characteristics of this data and some fuzzy rules. Subsequently, money laundering is detected intelligently using the optimal patterns produced in an adaptive neuro-diffuse inference system and finally it is determined if it is committing a crime.

Link Analysis Technique with a Shorter Modified Route

Chen Yunkai P, Mai Quanwe, Lu Zhengding[21], have proposed a link analysis technique that uses a modified shortest path algorithm to identify the strongest associations between two or more entities in a money laundering network.

Fourier Analysis

Young C. [22] performed Fourier analysis of a transactional account history in the time domain to construct a power spectrum that produces the magnitude of the movements of assets inside and outside the account as a function of frequency.

Suffix Tree of Probabilities to determine sequential anomalies.

The framework proposed by the authors Xuan Liu, Pengzhu Zhang, and Dajun Zeng[23], method combines sequence matching and classification methods and its divided in three steps:

The learning sequences are obtained using a probabilistic model which uses query sequences by selecting high risk sequences in the sequences of transactions.

Reference sequences are calculated, to obtain them the Euclidean distance is used to calculate similarities between the different sequences.

Then they use an algorithm created by them that consists of 4 stages (data acquisition and analysis, the selection of high-risk sequences, the calculation of similarity between the high-risk sequences and the reference sequences, and the classification of sequences), to classify sequences into normal and suspicious.

As you can see, artificial intelligence is used in this type of problem and has become a fundamental part of the fight against money laundering.

III. DEVELOPMENT

In this section a description of our proposal based on an expert system, its main objective is the evaluation of customer transactions by an algorithm with a decision tree approach and based on rules to identify if these are suspicious.

The architecture of the expert system is shown in the following figure: it is composed offourimportant points:

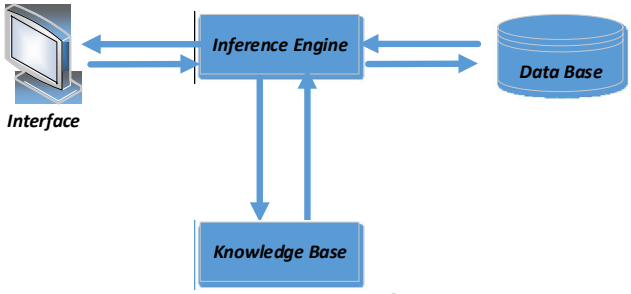

Fig. 1 Expert system architecture

A. Interface

It works as a link for the interaction between the user and the inference engine, this interface work on WEB and it is written in the php language.

In this interface, different variables are defined, which help the decision making of the inference engine.

B. Knowledge base

The knowledgebase (KB) is defined by:

$$KB = Rules \cup Facts \cup Func \cup MetaR$$

Rules. Norms that evaluate the data, and as a result throws zero or one, Rules = f (x) = {0,1}.Below is an example of a rule

tpo_categ == Salaried

Where:

tpo_categ.Is a variable assigned to receive the type of category that the client has.

Salaried. Is a constant

Facts. Rules with assigned values for example a value is assigned to a variable that in this case is id_account, and this is used by some rule.

id_account = 1

Where:

id_account. Is a variable which stores the identifier of the client's account.

Func. They are a set of instructions that are in the library of the rule handler in this case perform various tasks such as arithmetic, logic, counting or procedures, which return data or values. For example:

SUM ( )

Where :

SUM ( ) = function that performs the summation of the elements indicated within the parentheses.

MetaR. They control the operation of rules, for example the table 1 shows two rules which have an assigned order of execution and this is done for the resolution of conflicts or priorities that the user defines.

Table 1. Example of meta rules

Rule	MetaR
tpo_categ == Salaried	1
SUM (amount E account_id)	2

For the creation of the knowledge base, government documents and regulations were analyzed, reaching the conclusion that the regulations that the*Secretaría de Hacienda y CréditoPúblico* has published will be taken as a basis, since in one of the instances that participates in the prevention and fight against money laundering and financing of terrorism within the federal scope of Mexico.

C. Inference Engine

To have a better understanding of how the decision tree structure that is used[23] works for this research, we will begin with the following points:

- Root node
- Father Node
- Son Node

It is clear that the root of a tree is at the level 0R_{ini} from which n rules R_{ini}=> R_1, R_2,...,$R_n$can be derived, on the other hand the root node is also identified as having no rule that precedes it and is only .

On the other hand, any vertex$R_n$in the level k ≠ 0 is adjacent to a single vertex$R_w$of the previous level. The vertex$R_w$is called the father ofR_n, it returns the antecedent or generating rule of the R_n.

$$Father(R_n) = R_{ini}$$

In a similar way we say that$R_n$is the son of R_w, which returns, the descendant rule (s) of the ruleR_n

$$Son\ (R_{ini}) = \{R_n,\ldots,R_k.\}$$

Once this is understood, the structure must comply with the following premises for its proper functioning as mentioned in [23]:

- Set not empty

It means that the structure of the tree must not be an empty set of rule R_1, R_2, ...,$R_n$of the form:

$R_{ini} = Son\ (R_{ini}) = R_j$
$R_{ini} = Son\ (R_{ini}) = R_j$
$R_k = Son\ (R_j)$

$$R_n|Father\ (R_i) \cup R_i \cup Son\ (R_i)$$

WhereR_n represents rules, of the type: Metarelations, rules, concepts, facts or functions, necessary to be able to consider such rule as true.

- Reasoning line

Fulfilling the above, it is said that:

A sequence R_1, R_2, ..., $R_n$of elements is a line of reasoning, if it is fulfilled that for each R_i(i= *1; ... ; n-1*) some of its descendants represented by the function Son(R_i) appears also as part of the ancestor represented by the Father function (R_{i+1}) of the rule R_{i+1} . Formally, R = R_1, R_2,...,$R_n$is a line of reasoning if it is a finite set of ordered rules and complies with:

$$\forall R_i\ (1 \leq i > n) \in KB,\ \exists R_i \subset Rules \cup MetaR \mid R_i \subset Son\ (R_i) \wedge Father\ (R_{(i+1)})$$

Finally the structure of the tree arrives at a decision which is controlled by a rule handler which receives rules Ci and returns false or true being 1.

- Rules handler

The structure of this rules handler by Ramírez Romero [23] consists of 3 steps:

1. Representation of rules in the database
2. Rules evaluator algorithm
3. Algorithm SQL language constructor

1. Representation of rules in the database

In this section a table is created to store the rules with the tree structure as shown below:

Table II. Eexample of table with data

Father_rule	Value_rule	Son_rule	Id_group_rule	Order_rule
Beginning		con_cve		
con_cve	22	con_cve22		
con_cve22	tpo_categ ==Professional activities on their own	con_cve22_detalle	2	1
con_cve22_detail	tpo_categ	con_cve22_detail		
con_cve22_detail	==			

As you can see, it started with the parent rule con_cve which has an identifier 22, which will be responsible for executing the rule that is contained in this identifier.

In this example we only have tpo_categ == Professional activities on their ownfrom which three elements are derived, the first is a variable called tpo_categ which will be replaced by the element assigned by the user, then the second element is an equality operator == that will make a comparison with the last element of the rule that is a constant called Professional activities on their ownand the The result of the evaluation will be false or true {0,1}.

Also in the identifier 22 there are other rules that are shown in the following table.

Table III. Example of rules contained in identifier 22

1	con_cve22	antilavadop4.client	con_cve22_detail
2	con_cve22	tpo_categ ==Professional activities on their own	con_cve22_detail
3	con_cve22	SUM (amount E id_account C antilavadop4.regist)	con_cve22_detail
4	con_cve22	CALC (amount E id_account C antilavadop4.regist) > 4	con_cve22_detail

The rules that are contained in the previous table are described in a general way

1. Access the customers table of the antilavadop4 database
2. Compare the variable tipo_categ with the constant Professional activities on their own
3. Add the amount of the transferences made by a client
4. Counts the number of operations performed by a client

2. Rules evaluator algorithm

The algorithm includes a function called *eval* (C_i), which evaluates the parameters Ci, where the result is true if it is the value 1 and false if it is 0.

$$eval\ (C_i) = \{1,0\}$$

Where:

Ci are strings of text that make up the parameters provided by the user, and also a rule that indicates the place where the base of knowledge where the evaluation function *eval()* works, once this is done, the function proceeds to do an analysis syntactic content to later decompose and extract the necessary information.

To have a better idea of how C_i works we should be divided into two:

- A rule that indicates the place of the node of the knowledge base where it will work.

  This is located within the knowledge base and is managed under a variable called $cve_concept, which will take the value of

  $ concept_cve = 22

- Parameters provided by the user.

  The user provides the necessary data for the operation of the rules that will be evaluated.

  $ account_id = 2

  $ tpo_categ == Professional Activities by own account

Then the two components of Ci are saved in a variable in the form of a text string as shown below

$ condition = ¨ Rule: con_cve = 22, Var: $ account_id = 2, Var: $ tpo_categ == Professional activities on your own¨;

Finally this variable is sent to the eval() function eval ($ condition);
Function eval ( )

Once the condition variable is received, the variables are separated and stored in an array called $ arrays_vars and the rule's index in $ arrays_ rules.

Subsequently, with the location index stored in the variable $ array_fixes, it allows the function to determine the position of the rules to be executed that are in the knowledge base in this case the rules contained in

con_cve = 22

Identified, the rules are extracted and executed one by one according to the criteria of the $son\ (R_i)$ in a cyclical manner until the result is true.

The rule is extracted and its elements are stored in a variable called $elements_rule, and the variables $elements_rule, $array_vars, are sent to the function rule_particular ().

This function is responsible for determining the authenticity of the rule, returning as result 1 or 0. One of the tasks performed is to match the variables that are sent by the user with the variables that the rule needs for its operation, but if these do not match the process is terminated due to lack of information.

If the variables agree with the rules that are needed, a function is performed that determines the type of rule, which can be:

- comparison
  this includes the operators {<,>, <=,> =, <>, =}, and the variables to buy, resulting in false or true

Algorithm SQL language constructor

- related to database
  They are divided in two:

  Simple consultations

SELECT * FROM antilavadop4.clients WHERE account_id = 2

Which are true if there is at least one value extracted from this query otherwise it will be false.

Queries using functions COUNT (parameter), SUM (parameter), MAX (parameter), etc.

SELECT SUM (amount) FROM antilavadop4.regist WHERE id_account = 2;

This type of query will only return a numeric value.

Finally, the value obtained from the whole evaluation is returned to the function rule_particular () and gives a result of the evaluation of the rules.

D. Data Base

The knowledge generated and contained in the database is based on documents published by different institutions and on the other hand, the practical bases obtained in the development of the investigation with the purpose of giving a solution that is closer to reality.

The database consists of several tables below are some of them:

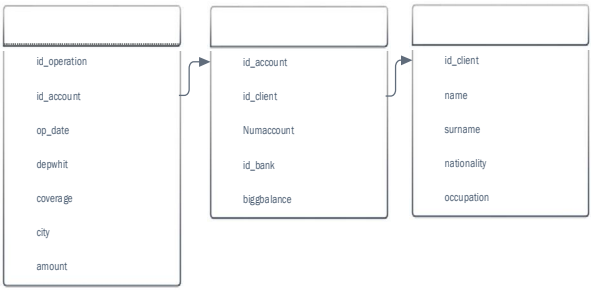

Fig. 2 Database tables

The tables contain records of banking transactions that were generated by a simulator, these records are used by the inference engine to understand, formulate and resolve if a client is committing an illegal act.

IV. EXPERIMENTATION AND RESULTS

To test the operation of the expert system, the following test was carried out, which has the following description:

Case 1.

Description:

It is a person who is a Family Father and resides in Morelos, which only has income from a third party.

With time, it is detected that it carries out money laundering activities by simulating income as a result of its legitimate activities; and by receiving and transferring funds abroad

Warning signs:

- Operations performed out of profile
- Fractional operations to bypass control systems
- Intensified use of cash
- Activities carried out in high risk areas

It is explained in a general way how the rules contained in table IV work, so that the rules contained in the knowledge base work correctly, several variables are needed.

These are entered by the system administrator through the interface, in this example of rules the variable tpo_categ is received, which contains the value of Parent, then the inference engine starts looking for each of the rules contained in the knowledge base and executes them.

For example, the first rule found by the inference engine is

Rule 1.tpo_categ == Salaried

Then the inference engine searches for the content of the variable tpo_categ, which is substituted in the rule.

Table IV Abstract of rules analyzed for this case

Rule	Rule broken course	Substituted rule:	Result
1	tpo_categ == Salaried	Parent == Salaried	0
2	tpo_categ == Professional activities for own account	Parent == Professional Activities for own account	0
3	tpo_categ == Business activities	Parent == Business activities	0
4	tpo_categ == Industrial activities	Parent == Industrial activities	0
5	tpocateg == Motor transport activities	Parent == Motor transport activities	0
6	tpo_categ == Parent	Parent == Parent	1
7	SUM (begbalance E id _ customer C antilavadop4.accounts)> 200000	206000> 200000	1
8	COUNT (amount E id _ account C antilavadop4.registroop)>5	11> 5	1
The final result of the evaluation of rules is: 1			

Rule 1.Parent == Salaried

Once having all the elements of the rule is evaluated, resulting in 0, because parent is not equal to salaried, as a result the inference engine executes the following rule.

As can be seen in table 1, rules 2 through 6 are similar and follow the same treatment except for rule 6 that results in 1, because

Rule 6.tpo_categ == Salaried

Then it makes the substitution:

Rule 6.Parent == Parent

And it is evaluated giving as a result 1, to which the inference engine proceeds to execute the rules that are children of that rule in this case executes rule 7.

Rule 7.SUM (begbalance and id_customer C antilavadop4.accounts)> 200000

Which contains these elements:

- Function SUM() that performs the summation of what is contained in it.
- Variable *begbalance* contains amounts from customer accounts and this data is extracted from the database.

- *E* means that it belongs to
- Variable *id_customer* is assigned through the interface by the system administrator.
- C means that it is contained in.
- *antilavadop4.accounts* is theorganization's database and the table where the data is contained.
- Comparison> 2000.

In other words, the rule makes the summation of the accounts that the client has contained in the database to then make the comparison, resulting in:

206000> 200000

Therefore, the evaluation gives 1 and continues with the following rule.

Rule 8. COUNT (city == strategic deficiency and id _ account C antilavadop4.registroop)> 5

It contains the following elements:

- Function Count ( ) performs the account of what is contained in it.
- Variable *City* contains data on cities that have strategic deficiency and those that do not.
- Comparison with the constant strategic deficiency.
- *E* means that it belongs to.
- Variable id _ customer is assigned through the interface by the system administrator.
- *C* means that it is contained in.
- antilavadop4.city is theorganization's database and the table where the data is contained.
- Comparison> 5.

In other words, the rule counts the transfers made to countries with strategic deficiency of the client contained in the database and then make the comparison, resulting in:

11> 5

Therefore giving the evaluation 1 and therefore the inference engine finds that there are no more rules to execute marks it as possible suspect of money laundering.

Case 2.

Description:

In this case, an organization that is dedicated to the Sale of Goods which is located in Hidalgo, México, in the last month has had income outside the country, which does not generate any warning signal because its operations are not outside the profile and its geographic area in which he works.

Signs:

- Operations performed within profile.
- Country income without strategic deficiency.
- Intensified use of cash.
- Sustainable transfers.

Table V
Abstract of rules analyzed for this case

Rule	Rule broken course	Substituted rule:	Result
1	tpo_categ == sale of goods	sale of goods == Salaried	0
2	tpo_categ == Professional activities for own account	sale of goods == Professional Activities for own account	0
3	tpo_categ == Business activities	sale of goods == Business activities	0
4	tpo_categ == Industrial activities	sale of goods== Industrial activities	0
5	tpocateg == Motor transport activities	sale of goods == Motor transport activities	0
6	tpo_categ == Parent	sale of goods == Parent	0
7	tpo_categ == sale of goods	sale of goods == sale of goods	1
8	SUM (begbalance E id _ customer C antilavadop4.accounts)> 200000	2030000> 2000000	1
9	COUNT (coverage == outside E id _ account C antilavadop4.registroop)> 4	0> 10	0
10	COUNT (depwhit == outside E id _ account C antilavadop4.registroop)	5 > 10	0
The final result of the evaluation of rules is: 0			

Now table 2 is explained:

The variable tpo_categ which contains the value of sale of goods, followed immediately by the inference engine executes the first rule.

Rule 1.tpo_categ == Salaried

Then the inference engine searches for the content of the variable tpo_categ, which is substituted in the rule and is as follows

Rule 1. Sale of goods == Salaried

Once having all the elements of the rule proceeds to evaluate, resulting in 0, because output of goods is not equal to salaried, as a result the inference engine executes the following rule.

As can be seen in table 1, rules 2 through 7 are similar and follow the same treatment except for rule 7 that results in 1, because:

Rule 7.tpo_categ == Sale of goods

Then he makes the substitution.

Rule 7. Sale of goods == Sale of goods

And it is evaluated giving as a result 1, to which the inference engine e proceeds to execute the following rules.

Rule 8. SUM (begbalance and id _ customer C antilavadop4.accounts)> 200000

Which contains these elements:

- Function SUM () that performs the summation of what is contained in it.
- Variable *begbalance* contains amounts from customer accounts and this data is extracted from the database.
- *E* means that it belongs to.
- Variable *id_customer* is assigned through the interface by the system administrator.
- *C* means that it is contained in.
- *antilavadop4.accounts* is the database of the organization and the table where the data are located.
- Comparison> 2000000.

In other words, the rule makes the summation of the accounts that the client has contained in the database to then make the comparison, resulting in:

2030000> 2000000

Therefore, the evaluation gives 1 and continues with the following rule.

Rule 9. COUNT (coverage == outside E id _ account C antilavadop4.registroop)> 4

It contains the following elements:

- Function Count () performs the account of what is contained in it.
- Variable coverage contains data on customer transfers abroad.
- Comparison with the constant outside.
- E means that it belongs to.
- Variable id _ customer is assigned through the interface by the system administrator.
- C means that it is contained in.
- antilavadop4.registroop is the database of the organization and the table where the data is contained.
- Comparison> 10.

The rule counts the transfers made abroad by customer contained in the database to then make the comparison, resulting in

0> 10

Therefore giving the evaluation 0 and consequently the inference engine proceeds to the next rule

Rule 10. COUNT (depwhit == outside E id _ account C antilavadop4.registroop)

It contains the following elements:

- Function Count () performs the account of what is contained in it.
- Variable depwhit contains data of transfers made from abroad to the client's account.
- Comparison with the constant outside.
- E means that it belongs to.
- Variable id _ customer is assigned through the interface by the system administrator.
- C means that it is contained in
- antilavadop4.registroop is the database of the organization and the table where the data is contained.
- Comparison> 10.

The rule counts the transfers made from abroad to the client contained in the database to then make the comparison, resulting in:

0> 10

The evaluation of the rules found in the knowledge base and the records contained in the database is concluded, resulting in the suspect of no money laundering.

V. CONCLUSION

Decision tree method is very flexible and powerful, as it is known that money laundering is very complex, because criminals look for different methods to transform illicit money into licit, and the use of this method allows us to add more rules when new methods emerge to circumvent the system.

The results showed that the client may be suspected of incurring in this illegal act through the system described in this article.

REFERENCES

[1] UIF. (2015). Obtenidode http://www.gob.mx/shcp/ documentos / shcp-unidad- de- inteligencia - financiera - uifJ.

[2] Governance, B. I. (2015). Obtenido de https://www.baselgovernance.org/publications.

[3] Patcha, A., & Park, J.-M. (2007). An overview of anomaly detection techniques: Existing solutions and latest technological trends. Computer Networks, 3448-3470. doi:dx.doi.org/10.1016/j.comnet.2007.02.001

[4] Gilmour, N. (2016). Understanding the practices behind money laundering – A rational choice interpretation. *International Journal of Law, Crime and Justice*, 1-13. doi:10.1016/j.ijlcj.2015.03.002

[5] Nan Wang, S., & Gang Yang, J. (2007). A Money Laundering Risk Evaluation Method Based on Decision Tree. *Sixth International Conference on Machine Learning and Cybernetics*, 19-22. doi: 10.1109/ICMLC.2007.4370155

[6] Quinlan, J. R. (1986). Induction of Decision Trees. *Machine Learning 1(1)*, 81–106. doi:10.1023/A:1022643204877

[7] Jayasree, V., & Siva Balan, R. V. (2016). Money Laundering Regulatory Risk Evaluation Using Bitmap Index-Based Decision Tree. *Journal of the Association of Arab Universities for Basic and Applied Sciences*. doi:10.1016/j.jaubas.2016.03.001

[8] R. Dre_zewski, J. S. (2012). System supporting money laundering detection. *Information Science*, 8–21.

[9] Gao, S., & Xu, D. (2009). Conceptual Modeling and Development of an Intelligent Agent-Assisted Decision Support System for Anti-Money Laundering. *Expert Systems with Applications*, 1493–1504. doi:10.1016/j.eswa.2007.11.059

[10] Wang, X., & Dong, G. (2009). Research on Money Laundering Detection Based on Improved Minimum Spanning Tree Clustering and Its Application. *Knowledge Acquisition and Modeling*, 62-64. doi:10.1109/KAM.2009.221

[11] Larik , A., & Haider, S. (2011). Clustering Based Anomalous Transaction Reporting. *Elsevier*, 606-610. doi:10.1016/j.procs.2010.12.101

[12] Raza, S., & Haider, S. (2011). Suspicious activity reporting using dynamic bayesian networks. *Procedia Computer Science 3*, 987–991. doi:10.1016/j.procs.2010.12.162

[13] Luo, X. (2014). Suspicious Transaction Detection for Anti Money Laundering. *International Journal of Security and Its Applications*, 157-166. doi:10.14257/ijsia.2014.8.2.16

[14] Hong, X., Liang, H., Gao, Z., & Li, H. (2016). An Adaptive Resource Allocation Model in Anti-Money Laundering System. *Springer Science*. doi:10.1007/s12083-016-0430-y

[15] Tao Lv, L., Ji, N., & Long Zhang, J. (2008). A RBF Neural Network Model for Anti-Money Laundering. *IEEE Computer Society*, 209-215. doi:10.1109/ICWAPR.2008.4635778

[16] Umadevi, P., & Divya, E. (2011). Money Laundering Detection Using TFA System. doi:10.1049/ic.2012.0150

[17] Dreżewski, R., Sepielak, J., & Filipkowski, W. (2014). The Application of Social Network Analysis Algorithms in a System Supporting Money Laundering Detection. *Information Science*, 18-32. doi:10.1016/j.ins.2014.10.015

[18] Shafea, T. H.-M., Hossam Moustafa, T., Abd El-Megied, M. Z., Salah Sobh, T., & Mohamed Shafea, K. (2015). Anti Money Laundering Using a Two-Phase System. *Journal of Money Laundering Control*, 304 - 329. doi:10.1108/JMLC-05-2014-0015

[19] Flores, D. A., Angelopoulou, O., & Self, R. J. (2012). Combining Digital Forensic Practices and Database Analysis as an Anti-Money. *Emerging Intelligent Data and Web Technologies*, 218-224. doi:10.1109/EIDWT.2012.22

[20] Heidarinia, N., Harounabadi, A., &Sadeghzadeh, M. (2014). An Intelligent Anti-Money Laundering Method for Detecting Risky Users in the Banking Systems. International Journal of Computer Applications, 35-39. doi:10.5120/17141-7780

[21] Yunkai, C., Quanwe, M., & Zhengding, L. (2006). Using Link Analysis Technique with a Modified Shortest.Path Algorithm to Fight Money Laundering. *Wuhan University Journal of Natural Sciences*, 1352-1356. doi:10.1007/BF02829265

[22] Young, C. (2014). Periodic Account Activity and Automated Money Laundering Detection. *Journal of Money Laundering Control*, 295-297. doi:10.1108/13685200310809707

[23] Ramírez Romero, T. A. (2013), Filtering the input data by production rules on open database, International Journal of Latest Research in Science and Technology, Volume 2, Issue 5; Page 1-8, September - October 2013