ISSN 1913-8989 E-ISSN 1913-8997
Published by Canadian Center of Science and Education

Ontology Based Expert-System for Suspicious Transactions Detection

Quratulain Rajput[1], Nida Sadaf Khan[1], Asma Larik[1] & Sajjad Haider[1]

[1] Faculty of Computer Science, Institute of Business Administration, Karachi, Pakistan

Correspondence: Sajjad Haider, Faculty of Computer Science Institute of Business Administration, Kiyani Shaheed Rd., Karachi 74400, Pakistan. Tel: 92-114-22-422. E-mail: sajjad.haider@khi.iba.edu.pk, sahaider@iba.edu.pk

Received: September 30, 2013 Accepted: November 20, 2013 Online Published: January 13, 2014

doi:10.5539/cis.v7n1p103 URL: http://dx.doi.org/10.5539/cis.v7n1p103

This research was partially supported by National ICT R&D Fund, Pakistan research grant number ICTRDF/TR&D/2010/06

Abstract

The development of an effective mechanism to detect suspicious transactions is a critical problem for financial institutions in their endeavor to prevent anti-money laundering activities. This research addresses this problem by proposing an ontology based expert-system for suspicious transaction detection. The ontology consists of domain knowledge and a set of (SWRL) rules that together constitute an expert system. The native reasoning support in ontology is used to deduce new knowledge from the predefined rules about suspicious transactions. The presented expert-system has been tested on a real data set of more than 8 million transactions of a commercial bank. The novelty of the approach lies in the use of ontology driven technique that not only minimizes the data modeling cost but also makes the expert-system extendable and reusable for different applications.

Keywords: ontology, expert system, suspicious financial transaction, anti-money laundering, outlier detection, description logic

1. Introduction

Money laundering is a process by which money obtained through illegal means is transformed into clean money. There are a number of diverse methods for money laundering such as tax evasion, illegal dealing of commodities, acquisition of loans via false information, money transfer under the head of fake business transactions, donation to fake charity organizations, etc. Acquiring an in-depth understanding of such methods for fighting back is a crucial part of all anti-money laundering (AML) activities (Chandola, Banerjee, & Kumar, 2009).

Financial institutions all over the world are enforced by governments to report suspicious activities. In this regard, these institutions use a variety of methods to identify suspicious activities such as activities identified by employees as they observe daily operations, law enforcement enquiries, and transactions of their customers (Ketkar, Shankar, & Banwet, 2013). They also analyze certain behaviors such as withdrawal/deposit of large amount of cash (above a specified threshold), domestic/foreign transactions, abnormal transactions considering the customer's past behavior, mode of transaction (cheque, cash, debit cards), etc. It is an established fact that many of the banks' strategies can easily be learned and dodged by money launderers. For example, in case of a large amount of transaction, a money launderer can decompose it into many small to medium amount transactions to make the activity unsuspicious. To counter these mischevious behaviors, we need an autonomous expert system that can quickly update its rule-base and can flag suspicious transactions (Wong, 2013).

In the past decade or so, researchers have been actively using ontology for knowledge representation in the fields of databases, information integration, cooperative information systems, information retrieval, electronic commerce, enterprise application integration, knowledge management, etc. (Hepp, Leenheer, de Moor, & Sure, 2008). This is primarily due to the fact that ontology makes the knowledge representation easily sharable and reusable. Beside domain knowledge, ontology also supports rules modeling which allows deduction of new knowledge. Among several rule languages, SWRL (Semantic Web Rule Language) is the most expressive language and has been standardized by the W3C community (Hitzler, Krotzsch, & Rudolph, 2009; Lavbic &

Bajec, 2012). The use of ontology in the development of an expert-system, therefore, becomes a natural choice as it not only incorporates the knowledge base but it also allows rule modeling; together they make an expert system easily reusable and independent from the operational data (Valiente-Rocha & Lozano-Tello, 2010). This paper presents an ontology based expert system for suspicious transaction detection. The use of ontology makes the system independent of domain knowledge as well as extensible if one wants to add ontologies of other domains.

The rest of the paper is organized as follows. Section 2 provides an overview of the related work while Section 3 explains the proposed ontology based expert-system for suspicious transaction detection. An application has been developed to understand the potential of the presented work and is discussed in Section 4. Finally, Section 5 concludes the paper and provides future research directions.

2. Related Work

The financial sector all over the world has shown significant improvement towards detection of suspicious transactions. The problem, however, is far from over and automated detection of variety of financial frauds is still a challenging task (Lewisch, 2008). From a historical point of view, the earlier anti-money laundering systems focused only on legislative considerations and compliance requirement which could easily be learned and evaded by money launderers (Gao & Ye, 2007). Recently, several suspicious transaction detection techniques have been developed that are based on machine learning techniques such as dynamic Bayesian Networks (Raza & Haider, 2011) and clustering (Larik & Haider, 2011). Despite the fact that the machine learning techniques help in acquiring hidden knowledge, the biggest challenge in their successful application is the training data requirement. Besides this, high computation requirement for model learning is another major concern. Finally, they are not necessarily the best choice when it comes to knowledge bases that are dynamic in nature (Webb, Pazzani, & Billsus, 2001). Chandola et al. (2009) have provided an extensive survey on the application of different machine learning techniques such as classification, clustering, nearest neighbor, etc. for anomaly detection. In the traditional (rule-based) expert-systems, on the other hand, knowledge engineers manually extract knowledge from human experts and make it part of the inference system. The performance of such expert-systems thus fully depends on the quality of the acquired knowledge-base and the inference engine. These expert-systems face a major challenge when operating in a dynamic domain as their anticipated inference capabilities are degraded with a continuously changing environment. In addition, in many cases there is no clear separation between the rule base and the inference engine which makes future modification quite cumbersome. Thus, there is a need of a system that can clearly separate the task of knowledge (rule) based updation from the inference engine. The semantic web technologies such as ontology (RDFS, OWL), rule language (SWRL), rule-engines (pellet, Hermit), ontology API (Jena), ontology editor (Portege) makes the realization of such expert systems possible (Hitzler et al., 2009; Lavbic et al., 2012). Recently, several ontology based expert systems have been proposed in the literature (Valiente-Rocha et al., 2010; Cheng, Du, & Ma, 2008; Fang, Fu, & Dong, 2007; Shue, Chen, & Shiue, 2009; Marwaha, 2012). In this paper, we have used semantic web technologies to build an ontology based expert system where the ontology consists of domain knowledge and rules which are independent from the inference system. The ontology knowledge base can be easily updated without any significant overhead and data storage requirement (Mehmet & Wijesekera, 2010; Ramaki, Asgari, & Atani, 2012).

3. Ontology Based Expert System for Suspicious Transaction Detection

This section explains the presented approach to detect suspicious financial activities by monitoring individual transactions. The expert-system utilizes ontology as well as rules for detecting suspicious transactions. The essential components of the presented approach, as shown in Figure 1, comprises of the following three major steps:

(i) Ontology construction

(ii) Ontology reasoning

(iii) Query on inferred ontology

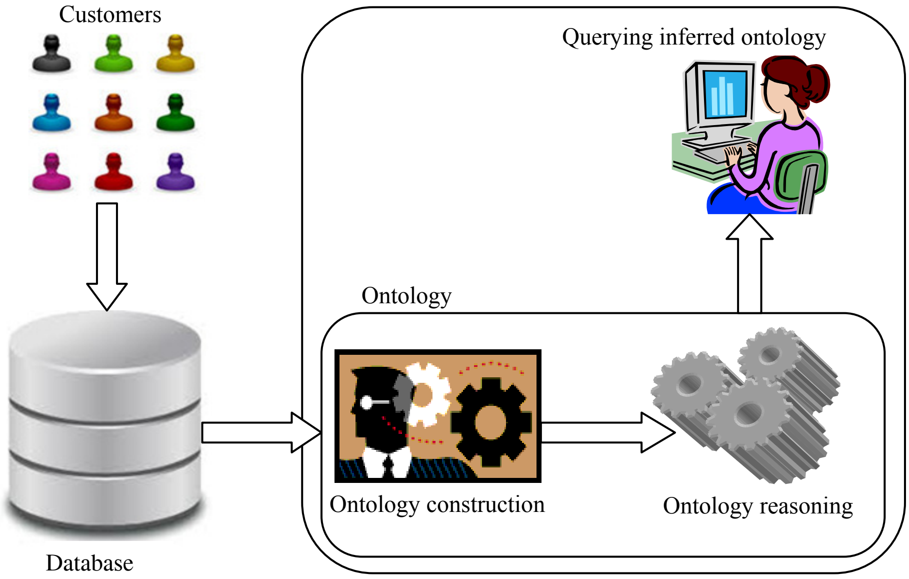


Figure 1. Components of ontology-based expert system

3.1 Ontology Construction

Ontology is used to develop an expert-system as it provides an unambiguous specification of knowledge and is adaptive in case of dynamic knowledge base. The ontology-based expert system consists of domain knowledge as well as some rules to support reasoning. Before constructing ontology, data pre-processing is required to select specific data items which can be transformed into the ontology. Figure 2 shows the ontology construction process. The following subsections explain different steps of the ontology construction process.

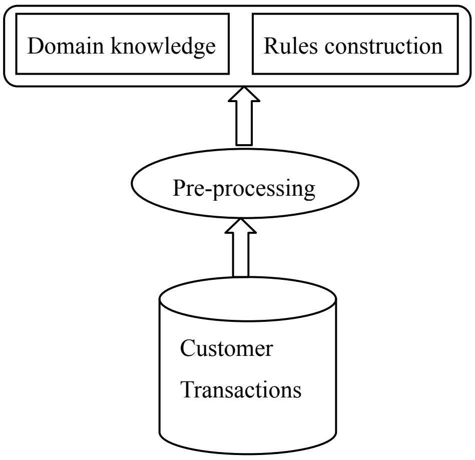


Figure 2. Ontology construction

3.1.1 Data Pre-Processing

Data pre-processing is an essential step in any information system as it eliminates the noisy data and performs data normalization. The presented approach in this paper uses Anti-Money Laundering guidelines provided by the State Bank of Pakistan as discussed later in the rules construction sub-section. To apply these guidelines we suggest to discard a transaction if it is below 100K PKR (approximately 1000 USD) as it is not deemed important for the purpose of money laundering. Furthermore, transactions are decomposed into groups of transactions as described by the following steps. A graphical representation of transactions' group distribution is shown in Figure 3 while few sample transactions updated after the application of the following steps are shown in Table 1.

i. Aggregate all transactions over intervals of 7-days and assign interval-ids to each aggregated values such as sum of debit transactions, sum of credit transactions, frequency of debit transaction and frequency of credit transaction.

ii. Select all records from step i where the sum of transactions (either debit or credit) amount is greater than or equal to 100000 PKR (1000 USD). This set of records belongs to group GT.

iii. Select all records from GT where the transaction is made by cheques only. This set of records belongs to group GC.

iv. Select all records from GT where the sum of transactions (either debit or credit) is greater than or equal to 500000 but less than 2500000. This set of records belongs to group GM.

v. For a particular account, if the difference between two consecutive transactions' interval-ids is greater than or equal to 24 (weeks) then the transaction belongs to a previously dormant account. Such observations belong to group GD.

Based on the above steps, new transactions are also easily decomposed into different groups.

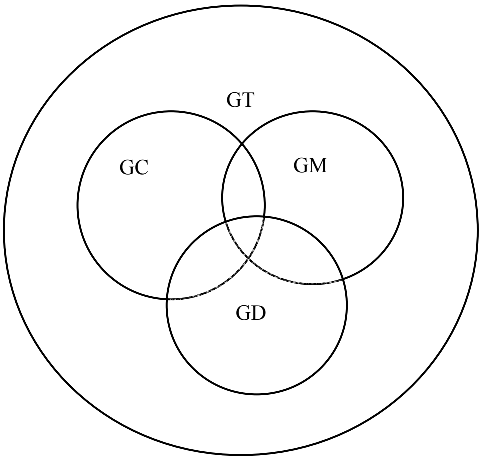


Figure 3. Transaction history decomposed into groups

Table 1. Pre-processed bank transaction data

Acct. No	Interval Id	Sum Credit Amount	Sum Debit Amount	Difference Amount	Sum Credit Freq Count	Sum Debit Freq Count	Group
1110	43	200000	424600	224600	1	1	GT, GM
11074	7	506400	180000	326400	1	1	GT,GC, GM
10388	2	1200000	1536680	336680	1	3	GT,GM

3.1.2 Domain Knowledge

The main purpose of the ontology is to store knowledge base of customers' transactions. This includes debit and credit transactions amount, their frequency in a given interval, etc. as computed in the preprocessing step. The knowledge base is built using several constructs of OWL (Web Ontology Language) such as class hierarchy, data type properties, object properties, domain range restrictions of each property and instances. Figure 4 shows the class hierarchy of transaction ontology while Table 2 lists the object properties and data properties with domain and range restrictions.

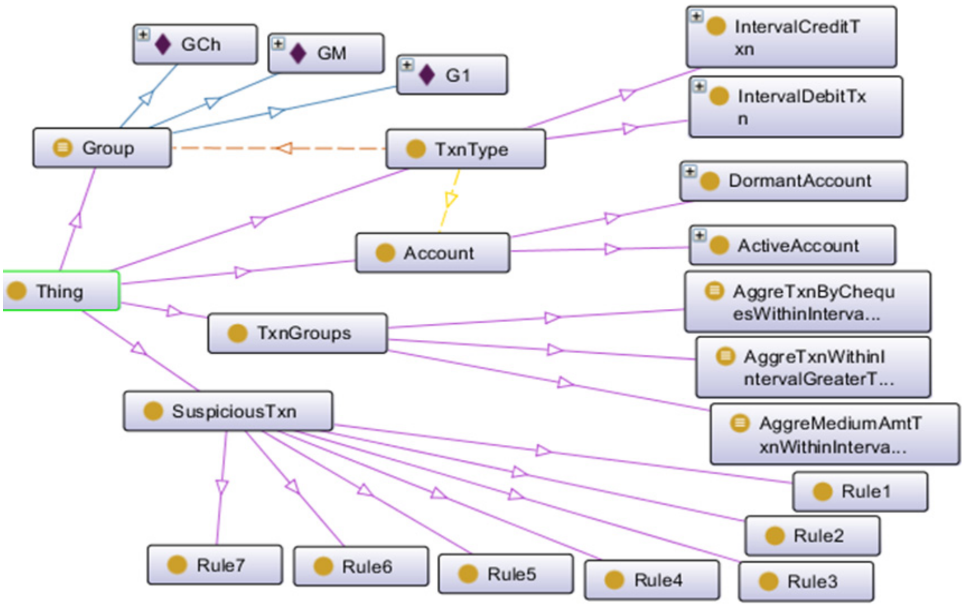


Figure 4. Class hierarchy of transaction ontology

Table 2. Properties of transaction ontology

	Property name	Domain	Range
Object Properties	belongsTo	TxnType	Group
	has Account	TxnType	Account
Data Properties	hasIntervalId	TxnType	nonNegativeInteger
	hasSumOfCreditTxnAmt	IntervalCreditTxn	nonNegativeInteger
	hasSumOfCreditTxnCount	IntervalCreditTxn	nonNegativeInteger
	hasSumOfDebitTxnAmt	IntervalDebitTxn	nonNegativeInteger
	hasSumOfDebitTxnCount	IntervalDebitTxn	nonNegativeInteger
	hasAccountNo	Account	nonNegativeInteger
	hasBeforeDormantInterval	DormantAccount	nonNegativeInteger
	hasAfterDormantInterval	DormantAccount	nonNegativeInteger

The conceptulization of customer's bank transactions as shown in Figure 4 helps in filtering out suspicious transactions. In general, there are two types of transactions: credit transactions and debit transactions. All instances of credit transactions are member of the *IntervalCreditTxn* class while all instances of debit transactions are member of the *IntervalDebitTxn* class. Each transaction is associated with Account which has an *AccountNo*. The class *Account* is further classified as *ActiveAccount* and *DormantAccount*. The class *Group* is defined as enumerated type in ontology with three possible instances: GT, GC, and GM. A transaction is assigned to these groups if it satisfies the criteria according to specified rules. The class *TxnGroups* shows the transactions membership according to assigned groups. All the transactions associated with group GT are member of subclass *AggreTxnWithinIntervalGreaterThan1Lac*, all transactions with group GC are member of subclass *AggreTxnByChequesWithinInterval*, and all transactions with group GM are member of *AggreMediumAmtTxnWithinInterval*. The *SuspiciousTxn* class hierarchy populates the transactions that are found suspicious based on pre-specified rules.

3.1.3 Rules Construction

The rules are built on top of the OWL ontology to deduce new knowledge (suspicious transactions) from the existing knowledge. The rules are presented in Semantic Web Rules Language (SWRL (Note 1)). To identify suspicious transactions, the rules are constructed using the anti-money laundering guidelines provided by the State Bank of Pakistan and completely/partially implemented by commercial banks within Pakistan. Table 3 provides a set of rules taken form the anti-money laundering guideline. It must be mentioned that the guidelines contain several rules for different types of financial services offered by banks such as customer business, personal loan, currency transfer abroad, etc. In this paper, we are focused only on customer transactions data therefore only transaction related rules have been selected from the guidelines. Table 4 shows the corresponding SWRL syntax.

Table 3. Rules for suspicious transaction detection

Rule#	Rule Description
1	A **large amount** of transaction is debited **immediately** after being credited to account.
2	A **dormant account** after activation starts transactions with **large amount**.
3	**Frequent** debit transactions of **large amount** through cheques.
4	A **dormant account** after activation starts debit transactions with **large amount**.
5	A **dormant account** after activation, receives series of amount until the sum is equal to **large amount** which is **immediately** debited.
6	A customer makes credit transactions that are less than **CTR filling threshold** while the sum is equal to a **large amount**.
7	A customer makes debit transactions that are less than **CTR filing threshold** while the sum is equal to a **large amount**.

The terms highlighted bold in Table 3 are defined as follows:

Large amount: amount that is greater than or equal to 2.5 million rupees (25,000 USD).

Immediately: within an interval of seven days.

Dormant account: no transaction history within 6 months.

Frequent: the frequency of transactions is greater than or equal to three within interval of seven days.

CTR filling threshold: Banks within Pakistan generate a CTR (Currency Transaction Report) if a transaction involves amount greater than 2.5 million rupees (25,000 USD).

It should be mentioned that the definitions of the above mentioned terms **Large amount, immediately, frequent** are not fixed. It is up to the financial monitoring unit to parameterized these values. In this paper, we have suggested the **large amount** as greater or equal to 2.5 million rupees as this amount is considered suspicious and worthy of CTR filing by the financial monitoring unit. To define the term **immediately**, we consider the time period of seven days as it is the smallest interval of time and can provide more closer look into changes in a customer‘s behavior. On the other hand, the term **frequent** defines the frequency of transactions within the interval of seven days. As the inerval is small therefore we suggest that greater than or equal to three should be considered as frequent. Finaly, the term **dormant account** and **CTR filing threshold** are standard terms and are defined by the financial monitoring unit.

Table 4. SWRL rules for suspicious transaction detection

Rule#	Rule Description
1	ActiveAccount(?Ac), IntervalCreditTxn(?CT), IntervalDebitTxn(?DT), TxnType(?T), BelongsTo(?CT, G1), BelongsTo(?DT, G1), hasAccount(?CT, ?Ac), hasAccount(?DT, ?Ac), hasAccount(?T, ?Ac), hasIntervalId(?CT, ?Cid), hasIntervalId(?DT, ?Did), hasSumOfCreditTxnAmt(?CT, ?CAmt), hasSumOfDebitTxnAmt(?DT, ?DAmt), equal(?Cid, ?Did), greaterThanOrEqual(?CAmt, 2500000), lessThanOrEqual(?Diff, 250000), subtract(?Diff, ?CAmt, ?DAmt) -> Rule1(?T)

2	DormantAccount(?Ac), TxnType(?T), BelongsTo(?T, G1), hasAccount(?T, ?Ac), hasAfterDormantInterval(?Ac, ?Dor_id), hasIntervalId(?T, ?id), hasSumOfCreditTxnAmt(?T, ?Amt), greaterThanOrEqual(?Amt, 2500000), greaterThanOrEqual(?id, ?Dor_id) -> Rule2(?T)
	DormantAccount(?Ac), TxnType(?T), BelongsTo(?T, G1), hasAccount(?T, ?Ac), hasAfterDormantInterval(?Ac, ?Dor_id), hasIntervalId(?T, ?id), hasSumOfDebitTxnAmt(?T, ?Amt), greaterThanOrEqual(?Amt, 2500000), greaterThanOrEqual(?id, ?Dor_id) -> Rule2(?T)

3	ActiveAccount(?Ac), TxnType(?T), BelongsTo(?T, GCh), hasAccount(?T, ?Ac), hasSumOfDebitTxnAmt(?T, ?Amt), hasSumOfDebitTxnCount(?T, ?c), greaterThanOrEqual(?Amt, 2500000), greaterThanOrEqual(?c, 3) -> Rule3(?T)
4	DormantAccount(?Ac), IntervalDebitTxn(?DT), BelongsTo(?DT, G1), hasAccount(?DT, ?Ac), hasAfterDormantInterval(?Ac, ?Dor_id), hasIntervalId(?DT, ?id), hasSumOfDebitTxnAmt(?DT, ?Amt), greaterThanOrEqual(?Amt, 2500000), greaterThanOrEqual(?id, ?Dor_id) -> Rule4(?DT)
5	DormantAccount(?Ac), IntervalCreditTxn(?CT), IntervalDebitTxn(?DT), TxnType(?T), BelongsTo(?CT, G1), BelongsTo(?DT, G1), hasAccount(?CT, ?Ac), hasAccount(?DT, ?Ac), hasAccount(?T, ?Ac), hasAfterDormantInterval(?Ac, ?Dor_id), hasIntervalId(?CT, ?id), hasIntervalId(?DT, ?id), hasSumOfCreditTxnAmt(?CT, ?CAmt), hasSumOfCreditTxnCount(?CT, ?F), hasSumOfDebitTxnAmt(?DT, ?DAmt), greaterThanOrEqual(?F, 2), lessThanOrEqual(?Diff, 250000), lessThanOrEqual(?IntDiff, 2), subtract(?Diff, ?DAmt, ?CAmt), subtract(?IntDiff, ?id, ?Dor_id) -> Rule5(?T)
6	ActiveAccount(?Ac), IntervalCreditTxn(?CT), BelongsTo(?CT, GM), hasAccount(?CT, ?Ac), hasSumOfCreditTxnAmt(?CT, ?Amt), greaterThanOrEqual(?Amt, 2500000) -> Rule6(?CT)
7	ActiveAccount(?Ac), IntervalDebitTxn(?DT), BelongsTo(?DT, GM), hasAccount(?DT, ?Ac), hasSumOfDebitTxnAmt(?DT, ?Amt), greaterThanOrEqual(?Amt, 2500000) -> Rule7(?DT)

3.2 Ontology Reasoning

Once the ontology is constructed along with rules, reasoning is applied on the new records/cases. Reasoning is a process of deriving new knowledge that is not explicitly expressed in the knowledge base. The SWRL rules expressed rules in term of OWL concepts and properties to provide more powerful deductive reasoning capabilities. The process can be performed with the help of either of the several available built-in reasoning engines such as Hermit, Pellet, Racer, Jess etc. In this paper, we have used Pellet reasoning engine. Figure 5 shows the reasoning architecture.

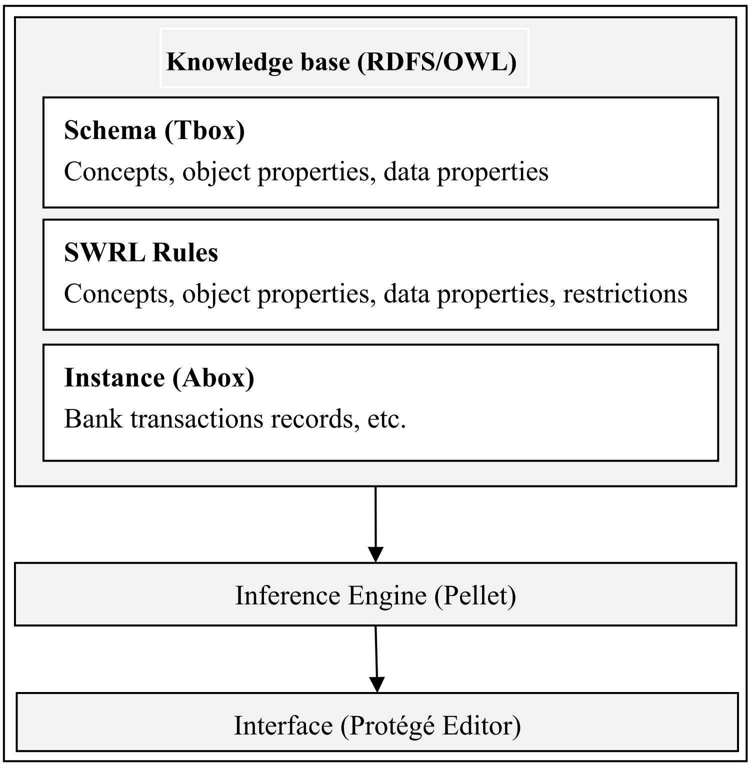

Knowledge base (RDFS/OWL)
Schema (Tbox)
Concepts, object properties, data properties
SWRL Rules
Concepts, object properties, data properties, restrictions
Instance (Abox)
Bank transactions records, etc.
Inference Engine (Pellet)
Interface (Protégé Editor)

Figure 5. Reasoning architecture

The knowledge base is processed by the reasoning engine and it identifies transactions that satisfy a rule(s). Such bank transactions are populated in a class hierarchy, named as *suspiciousTxn*. It must be noted that the inferred transactions are not mutually exclusive and it is possible that one transaction may satisfy more than one rule and thus become a member of multiple rule classes. The inferred ontology, shown in Figure 6, lists few transactions that are inferred member of SuspiciousTxn class.

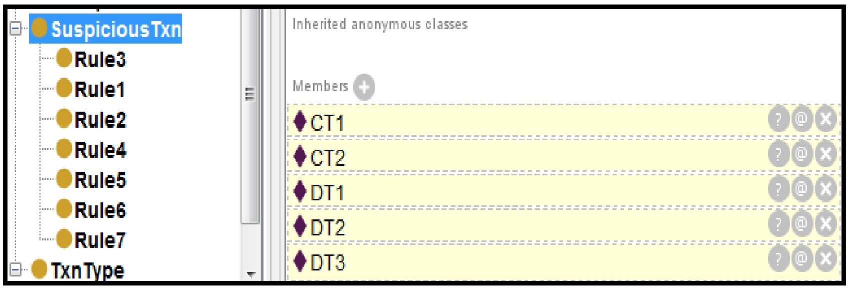


Figure 6. Inferred membership of SuspiciousTxn class

To understand the reasoning process, consider the following instance of a transaction after pre-processing step. First we populate this instance of bank transaction in ontology concepts and properties.

Acct No	Interval Id	Sum Credit Amount	Sum Debit Amount	Difference Amount	Sum Credit Freq Count	Sum Debit Freq Count	Group
12222	35	3000000	2500000	500000	1	2	GT

It is important to mention that Interval id is used to identify whether the given account is dormant or active. For example, if the difference in interval ids of same account is greater than 24 then the account is dormant. For the purpose of this example, we assume that this account is a dormant account. After entering the instance in the ontology, we run SWRL based inference engine to perform reasoning. The inference engine infers the class membership as deduced by the rules. Figure 7 shows the snapshot of the inferred knowledge in Protégé editor. This instance of bank transaction satisfies Rule2, Rule4 and Rule5 and as such becomes a member of SuspiciousTxn class that is a superclass of all these rules classes. Thus, the transaction is highlighted as suspicious transaction for further investigation.

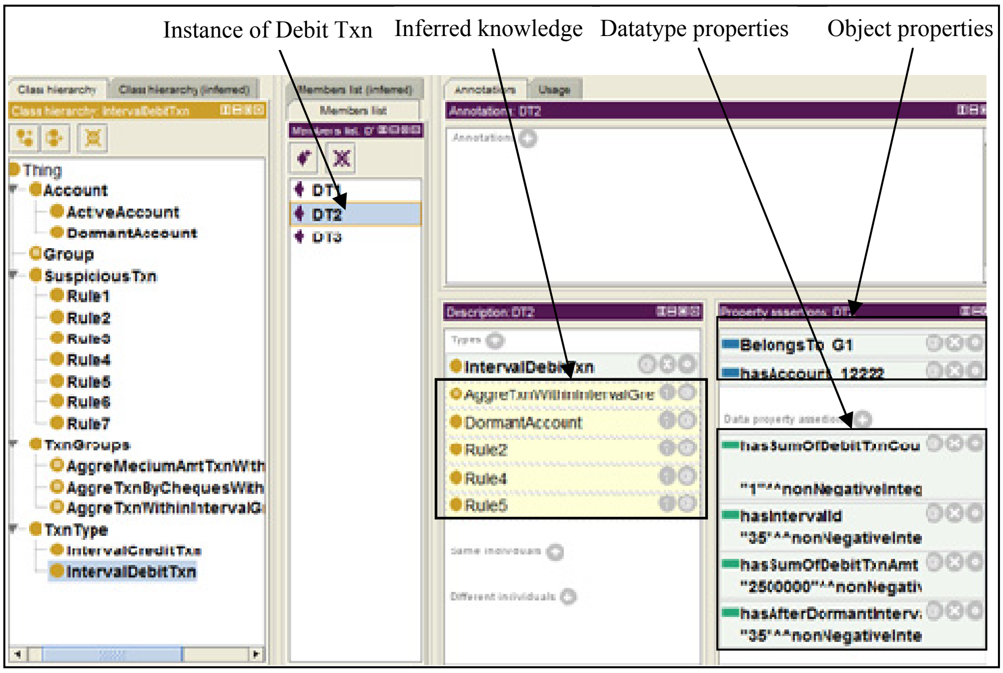
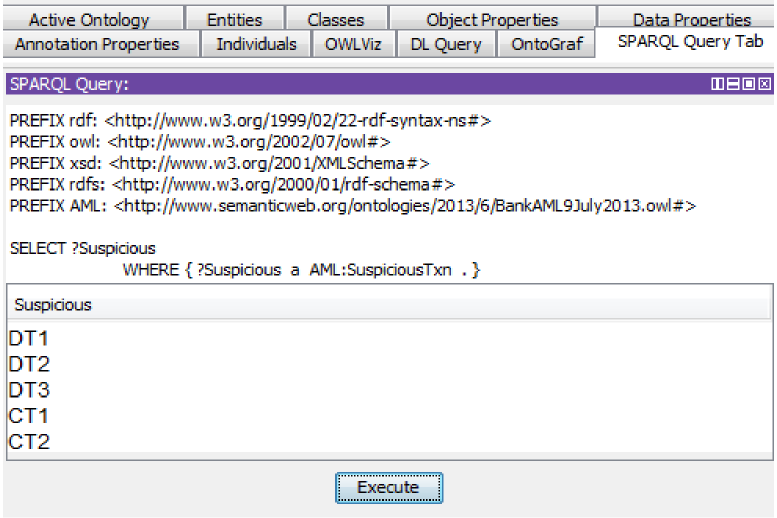


Figure 7. Inferred transaction membership in Rules classes

3.3 Query on Inferred Knowledge

Once the inference engine populates the *SuspiciousTxn* class hierarchy, we can query these transactions to get different type of information. The query is performed via SPARQL (Note 2) which is a standard query language to query ontology. Figure 8 shows an example of a SPARQL query that lists all transaction detected as suspicious while Figure 9 shows an example in which SPARQL query lists all transaction that satisfy Rule2. The CT1, CT2, and CT3 transactions in the figures are credit transaction while DT1, DT2, DT3 are debit transactions.

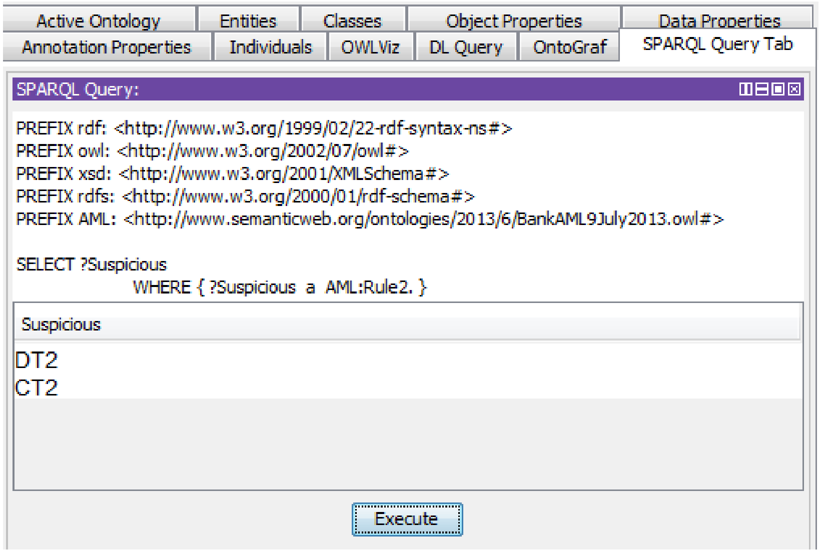


```
PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
PREFIX owl: <http://www.w3.org/2002/07/owl#>
PREFIX xsd: <http://www.w3.org/2001/XMLSchema#>
PREFIX rdfs: <http://www.w3.org/2000/01/rdf-schema#>
PREFIX AML: <http://www.semanticweb.org/ontologies/2013/6/BankAML9July2013.owl#>

SELECT ?Suspicious
            WHERE { ?Suspicious  a  AML:SuspiciousTxn  . }
```

```
Suspicious
DT1
DT2
DT3
CT1
CT2
```

Figure 8. Query to list all suspicious transaction



```
PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
PREFIX owl: <http://www.w3.org/2002/07/owl#>
PREFIX xsd: <http://www.w3.org/2001/XMLSchema#>
PREFIX rdfs: <http://www.w3.org/2000/01/rdf-schema#>
PREFIX AML: <http://www.semanticweb.org/ontologies/2013/6/BankAML9July2013.owl#>

SELECT ?Suspicious
            WHERE { ?Suspicious  a  AML:Rule2. }
```

Suspicious
DT2
CT2

Figure 9. Query to list transactions that satisfy Rule2

4. Application Development of the Ontology Based Expert-System for Suspicious Transaction Detection

The transaction knowledge base is modeled in ontology (OWL) using Protégé. Jena API is used to populate customer transactions in ontology. The future bank transactions will be populated in the ontology to identify suspicious transactions as discussed in the previous section.

To explain the working of the proposed system described in the previous section, here we test the system on a real data set. The data set contained 100K bank customers incurring 8.2 million transactions over the period of a year. The pre-processing step removed small amount transactions and as a result we ended up with a total of 214062 transactions. Among these transactions, the presented expert-system suggested 2% of the transactions as suspicious. It is important to note that the purpose of the presented system is to act as a decision-support tool and the final decision rests with the decision maker (typically the compliance head in this case) to consider a transaction as suspicious or not.

The main reason for this reliance on the compliance head is that despite the availability of real transactions, we cannot automatically validate that the transactions declared suspicious by our system are indeed suspicious as we do not have the required suspicious/non-suspicious labeling in our data set. However, it must be mentioned that the rules are developed by financial institutes and regulatory bodies based on their overall experience in dealing with suspicious transactions. As such, these rules have a high chance to filter suspicious transactions. The presented approach suggests that the use of ontology makes the expert system more efficient and reusable. In addition, modification/extension in the knowledge base and the rules base, when new customer behavior is found, is quite straight forward.

5. Conclusion

Financial institutions are enforced by the central banks and other regulatory bodies to have a proper anti-money laundering system in place that can report suspicious activities. The development of a fully automated mechanism to counter money-laundering activities is still a big challenge. However, various heuristics based AML guidelines are available that are being used by the several commercial banks. This paper proposed ontology based expert system to detect suspicious transactions. The use of ontology makes the expert system more efficient as it requires less computation and is able to reuse knowledge base in different applications across similar domain. The proposed ontology consists of transactions knowledge base and rules written in SWRL. We have used Pellet reasoner to deduce new knowledge about the nature of a financial transaction. We have analyzed our presented system on a real data set of 8.2 million transactions belonging to a commercial bank. The results show that the system is capable of suggesting transactions that can be further analyzed by the head of compliance department to label transactions as suspicious or not. In the future, we aim to apply the system in a bank to further analyze its strength to identify suspicious transactions.

References

Chandola, V., Banerjee, A., & Kumar V. (2009). Anomaly detection: A survey. *ACM Computing Surveys, 41*(3), 1-58. http://dx.doi.org/10.1145/1541880.1541882

Cheng, G., Du, Q., & Ma, H. (2008). The design and implementation of ontology and rules based knowledge base for transportation. *International Conference on Computer Science and Software Engineering, 3*, 1035-1038.

Fang, L., Cai, M., Fu, H., & Dong, J. (2007). Ontology-based fraud detection. *Computational Science ICCS* (pp. 1048-1055). Springer.

Gao, Z., & Ye, M. (2007). A Framework For Data Mining-Based Anti-Money Laundering Research. *Journal of Money Laundering Control, 10*(2), 170-179. http://dx.doi.org/10.1108/13685200710746875

Hepp, M., Leenheer, P., de Moor, A., & Sure, Y. (2008). Ontology management: semantic web, semantic web services, and business applications. *Semantic Web and Beyond, Vol. 7*. Springer. http://dx.doi.org/10.1007/978-0-387-69900-4

Hitzler, P., Krotzsch, M., & Rudolph, S. (2009). *Foundations Semantic Web Technologies*. Chapman & Hall/CRC.

Ketkar, S. P., Shankar, R., & Banwet, D. K. (2013). Telecom KYC and mobile banking regulation: An exploratory study. *Journal of Banking Regulation Advance online publication*. http://dx.doi.org/10.1057/jbr.2013.1

Larik, A. S., & Haider, S. (2011). Clustering based anomalous transaction reporting. *Procedia Computer Science, 3*, 606-610. http://dx.doi.org/10.1016/j.procs.2010.12.101

Lavbic, D., & Bajec, M. (2012). Employing Semantic Web technologies in financial instruments trading. *International Journal on New Computer Architectures and Their Applications (IJNCAA), 2*(1), 167-182.

Lewisch, P. (2008). Money laundering laws as a political instrument: the social cost of arbitrary money laundering enforcement. *European Journal of Law and Economics, 26*(3), 405-417. http://dx.doi.org/10.1007/s10657-008-9073-7

Marwaha, S. (2012). Ontology based Expert System. Development of Expert System in Agriculture, Indian Agricultural Statistics Research Institute (ICAR). Retrieved from http://www.iasri.res.in/ebook/expertsystem_o/Home.htm

Mehmet, M., & Wijesekera, D. (2010). Ontological Constructs to Create Money Laundering Schemes, Proceedings of the Fifth International Conference on Semantic Technologies for Intelligence, Defense, and Security, George Mason University.

Ramaki, A. A., Asgari, R., & Atani, R. E. (2012) Credit card fraud detection based on ontology graph. *International Journal of Security Privacy and Trust Management (IJSPTM), 1*(5), 1-12. http://dx.doi.org/10.5121/ijsptm.2012.1501

Raza, S., & Haider, S. (2011). Suspicious activity reporting using dynamic bayesian networks. *Procedia Computer Science, 3*, 987-991. http://dx.doi.org/10.1016/j.procs.2010.12.162

Shue, L. Y., Chen, C. W., & Shiue, W. (2009). The development of an ontology-based expert system for corporate financial rating. *Expert Systems with Applications, 36*(2), Part 1, 2130-2142. http://dx.doi.org/10.1016/j.eswa.2007.12.044

Valiente-Rocha, P. A., & Lozano-Tello, A. (2010). Ontology-based expert system for home automation controlling. *Trends in Applied Intelligent Systems* (pp. 661-670). Springer. http://dx.doi.org/10.1007/978-3-642-13022-9_66

Webb, G. I., Pazzani, M. J., & Billsus, D. (2001). Machine Learning for User Modeling. *User Modeling and User-Adapted Interaction, 11*(1-2), 19-29. http://dx.doi.org/10.1023/A:1011117102175

Wong, L. (2013). Money-laundering in Southeast Asia: liberalism and govern mentality at work. *Contemporary Politics, 19*(2), 221-233. http://dx.doi.org/10.1080/13569775.2013.785832

Notes

Note 1. http://www.w3.org/Submission/SWRL/

Note 2. http://www.w3.org/TR/rdf-sparql-query/

Copyrights