An Ontology-Based Alert Model for Financial Fraud Detection

Kainat Ansar, Mansoor Ahmed, Abid Khan

Islamabad 44000, Pakistan

Abstract
The objective of this research is to develop an effective model to detect financial fraud for the sustainable development of banks and financial institutes. Financial fraud is an issue which has a deep impact on the ordinary consumer as well as the finance industry. Our dependence on internet banking has grown far beyond our imagination and has made this problem more compound. Financial sector all over the world shows significant improvements in fraud detection. Fraud detection is a reactive response to misappropriation of financial results, which causes incurring cost that may or may not be recoverable due to fraud that has already occurred. However, the problem for automatic fraud deterrence is still a challenging task. Our focus in this work is on fraud deterrence. Deterrence is a proactive, preventative measure, which prevents loss before happening. We have proposed an ontology-based alert model for money laundering deterrence. We have also proposed an Intimation Rule Based (IRB) alert generation algorithm which stops fraud before it happens. This article first introduces the data representation model (ontologies) and the advantages of using ontologies over databases. Then we briefly discuss our proposed methodology and system working of our ontology-based alert model. We also evaluate our ontology using OntoClean methodology and compare results with existing techniques. Finally, the comparison results show that our system outperforms the existing systems.

Keywords:
Ontology-Based Alert, Fraud Detection; Ontology; Suspicious Transactions; Alert Model; Knowledge Base; Jena

.

1. Introduction

The process of turning illegally obtained currency into legal currency is called money laundering. Financial institutions are using different methods to record and report suspicious activities. These activities include daily observations from the employees for daily operations, customers transactions. Moreover, analyzing the certain behavior (i.e. deposit/withdrawal of large amounts, abnormal transactions, mode of transaction, foreign/domestic transactions) of the customers, researchers have proposed different approaches to resolve this problem (Dal, 2018). Moreover, for fraud detection, several data mining based techniques has been analyzed and practiced in recent years (Zhou, 2018). Despite adopting these techniques still, fraudsters find loopholes and somehow learn and dodge the system. For example, if the suspicious activities are monitored based on the transfer of large amounts, they might break the transaction into smaller units and achieve their target. Regardless of the economic circumstances, age or health, almost everyone needs banks for financial transactions. Research is going on to maintain users trust in the financial sector since long. A basic reason for fraud or deception is to get financial benefit in any form or shape like money laundering, credit cards, fake insurance claims for health or vehicle, etc. User behaviors, out of pattern activities, social analysis, data mining and statistical analysis of patterns are being used to detect and prevent such financial frauds. Because it is a continuously evolving discipline, therefore nothing is ultimate. Fraud detection techniques are explored with reference to financial fraud, telecommunication frauds, health care fraud and insurance fraud (Abdallah, 2016). Financial fraud could be of any type. Fig. 1 shows common types of financial frauds (West, 2016).

To develop an efficient system for suspicious transaction detection and fraud deterrence system is a critical problem. Such a system is needed that can quickly generate alerts on suspicious transactions and stops fraud. However, in this work, an ontology-based alert model is presented for money laundering deterrence. This model generates alerts on suspicious transactions with a corresponding severity level as discussed later in section 4.

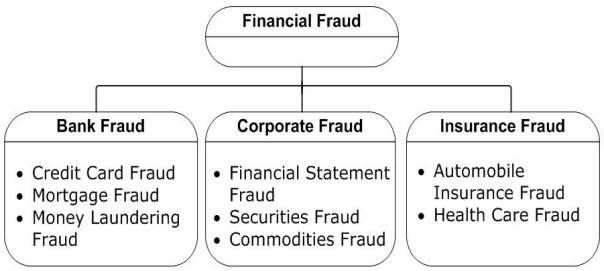

Fig. 1: Types of Financial Frauds

1.1. Ontologies versus Databases

Ontology is the best way to represent knowledge in a dynamic environment because it makes knowledge easily shareable and reusable. Additionally, ontology describes the terms, vocabularies, relationships and rules of the domain. It also describes knowledge in a generic way. Moreover, the ontology also supports reasoning in which the knowledge base sends inferred knowledge to the

Manuscript received June 5, 2025
Manuscript revised June 20, 2025
https://doi.org/10.22937/IJCSNS.2025.25.6.19

inference engine and adding some rules to the reasoning logic. So, using ontologies, we not only reduce the modeling cost but can also extend and reuse the ontology-based models in different applications within or across the domain. There are two major data representational models i.e. databases and ontologies. The relational database models have been in use for quite some time for storing and querying the data. However, on the other hand, ontologies have appeared as an alternate to databases with more enriched meaning. Ontology makes knowledge easily shareable and reusable (Dadjoo, 2015). Moreover, some of the advantages of using ontologies over databases are presented. Databases are usually designed for a specific application. For every new application, we must design a new database. Whereas on the other hand, ontologies which describes the concepts and their relationship in a specific domain can be re-used in different applications (within or across the domain) as per requirement. Additionally, ontologies help us to express the semantics in a much better and powerful way as compared to types and constraints in databases. However, database models do not permit the creation/addition of new records until and unless it does not satisfy the restriction of a particular table. Whereas on the other hand, reasoning/inferring capability in ontologies make it possible to produce new knowledge (i.e. new instances can be created even if they do not satisfy the restriction of any class). Also, one can map ontology's classes to database's tables, ontology's properties to database's attributes and ontology's axioms to database's constraints (Martinez-Cruz, 2012).

1.2. Motivation

Rajput et al. (2014) proposed an ontology-based system for fraudulent transaction detection. A hybrid data mining complex network classification algorithm for credit card fraud detection has been presented by Zanin et al. (2018). In this study, authors focused on fraud detection (which is a reactive response to misappropriation of financial results, which causes incurring cost that may or may not be recoverable due to fraud that has already occurred). However, our focus in this research work is on fraud deterrence. In addition to fraud detection, our proposed ontology-based system performs fraud deterrence as well. Reasoning capabilities in our ontology-based systems make it possible to derive facts that are not described in the knowledge base clearly. Moreover, from inferred transactions, this system has introduced alert severity level and dead alerts exclusion mechanism (which does not exist before) makes our system faster.

1.3. Our Contribution

In this work, we have proposed an ontology-based alert model for Financial Fraud Detection (FFD) and fraud deterrence. However, Main contributions of this research work are:

(i) Creating a comprehensive (having 40 classes + subclasses) FFD ontology from scratch. Describing the concept of customer's bank transactions and their relationships, ontology helps in finding suspicious transactions;
(ii) Developing Jena rules using apache Jena semantic web framework, for fraud alert systems;
(iii) Proposed ontology-based alert model with additional features, for money laundering deterrence;
(iv) Proposed IRB alert generation algorithm (which stops fraud before it happens). As the algorithm is shown in the subsequent section.

However, the rest of the paper is structured as Section 2 presents related work. In Section 3, types of fraud are explored. Furthermore, explanation of the system model and problem the formulation is discussed in Section 4. In addition, ontology construction methodology is presented in Section 5. Moreover, formal representation of FFD ontology is discussed in the subsection of Section 5. Section 6 and Section 7 presents ontology implementation and validation respectively. The evaluation setup, results and discussion are presented in Section 8. Finally, Section 9 presents the conclusion.

2. Related Work

With the advent of technologies and user's dependence on computing systems followed by automated and unattended authentications, increased financial deception cases. However, a lot of fraud detection techniques have been analyzed and practiced in recent years. Fig. 2 shows the detailed taxonomy of fraud detection techniques reviewed in this paper. Moreover, the summary of related work is shown in Table I.

Fraud prevention and fraud detection are two different aspects of a financial system. Prevention is the first layer, whereas detection is the next layer of protection to secure the system against fraud (Abdallah, 2016). Fraud detection techniques have been explored (West, 2016) with reference to credit card fraud, financial statement, insurance, securities and commodities fraud. Metadata provides basic public information about an object. Using meta-learning approaches with other classifier techniques to detect fraudulent activities in terms of ”misclassification” and ”correct classification” is addressed by Sen et al. (2013). Fraud can be categorized as behavioral fraud, application fraud, bankruptcy fraud and theft fraud (Delamaire, 2009). Frauds can be detected using supervised methods (classification) and un-supervised methods (behavior

changes or unusual transactions). These types of financial practices are discussed by Lata et al. (2015). Importance of data mining methods for fraud detection cannot be denied in any case.

Using different data mining techniques and amalgamation of different data mining techniques may return exponentially useful results. Nami et al. (2018) proposed a two-stage method based on random forest and K-Nearest Neighbor (KNN) for payment card fraud detection. An algorithm based on reverse KNN (method of classification) for credit card fraud detection is proposed in (Ganji, 2012). In data mining situations, unsupervised learning method (peer group analysis) is used for monitoring the behavior of a user over time. Similarly, Self-Organizing Maps (SOM) is suggested. Zaslavsky et al. (2006) developed a credit card fraud detection system using the SOM algorithm. This method detects changed behavior from previous practices of individuals. A fuzzy rule-based expert system is proposed by HaratiNik et al. (2012) for credit card fraud detection. Fuzzy rules are used for removing logical conflicts. In the field of internet banking, an intelligent system for user's abnormal behavior detection has been developed (Alimolaei, 2015). This system is based on fuzzy theory.

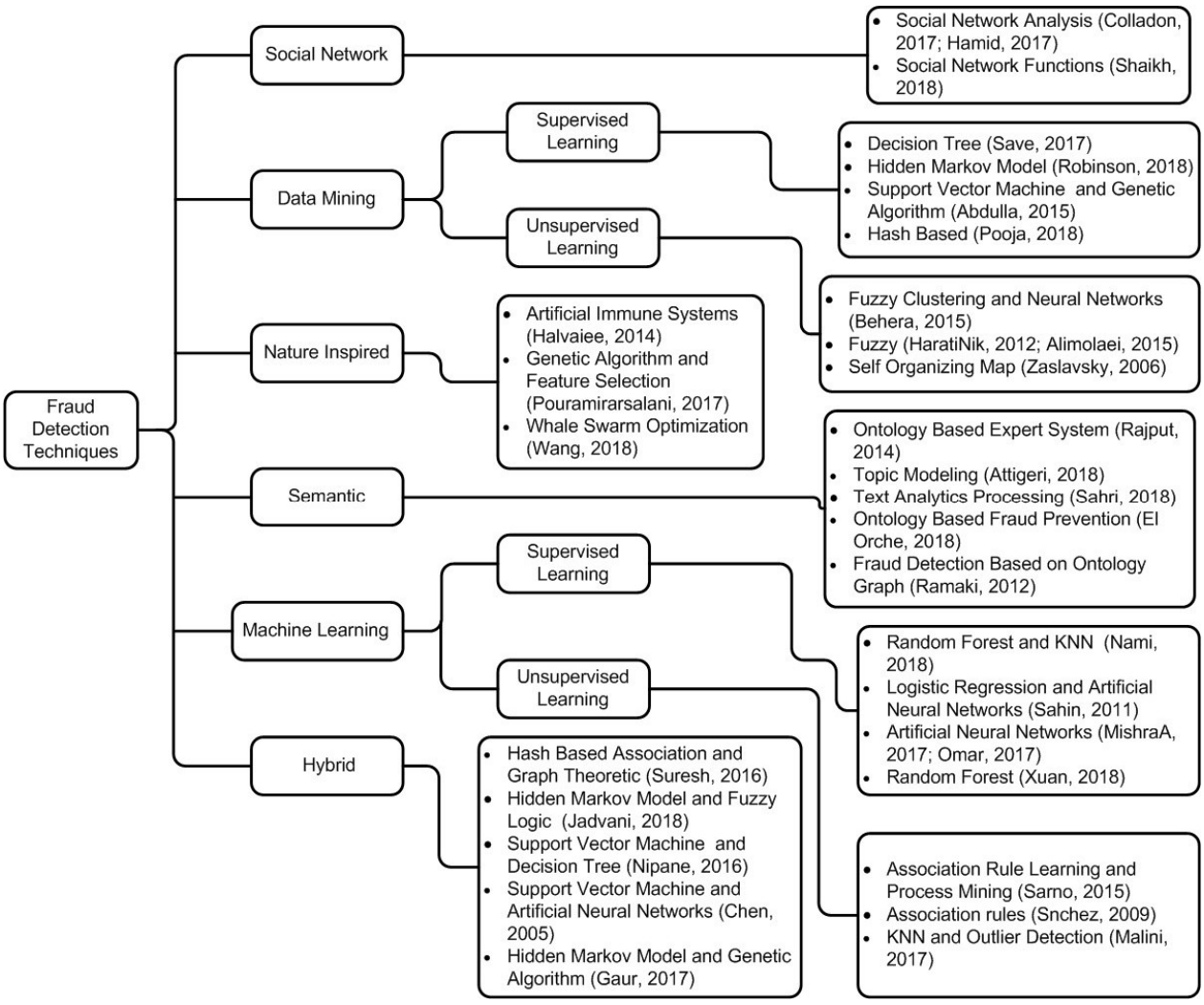

Fig. 2: Taxonomy of Literature Review

Moreover, data mining based, supervised learning methods are used by authors in recent years. Save et al. (2017) developed a system for Credit Card (CC) fraud detection. System is based on a decision tree with the integration of Luhn's and Hunt's algorithm. A system (based on hidden markov model) has been developed by Robinson

(Robinson et al., 2018) that performs automatically fraud detection in prepaid cards. This approach is tested on the real transaction data. Furthermore, several unsupervised learning techniques (Makki, 2017) are used for fraud detection in financial sectors.

Similarly, support vector machine, random forest, logistic regression and KNN are data mining approaches. Machine learning and data mining methods for CC fraud detection is discussed (Patil, 2018) by focusing real-life data of transactions from credit card operation. Data mining helps in detecting the wrong transactions. A first hybrid data mining/complex network classification algorithm has been presented (Zanin, 2018) for credit card fraud detection. Quah et al. (2008) proposed an innovative approach. The whole focus is based on real-time detection. With the combination of Genetic Algorithm (GA) and Support Vector Machine (SVM), a fraud detection system is proposed (Abdulla, 2015). GA performs feature selection, while SVM modeled for classification. This system is tested on UCSD-FICO Data mining contest 2009 data set. Frauds related to insurance claims of automobiles are reported frequently these days. Furlan et al. (2011) proposed a method (tool) for improvement of the fraud management process in vehicle insurance corporation. Similarly, Artificial Intelligence (AI) has an established impact on machine learning approaches. Topological data analysis can help in financial fraud detection using case-based reasoning, where a data bank is populated with well-known financial practices. This data bank cases can be added or withdrawn from time to time (Wasilewska, 2004). Solutions of problems of dataset imbalance, a framework is proposed (Zareapoor, 2017). This approach is tested on the real-time data provided by FICO.

In addition to supervised learning methods for fraud detection, graph mining hybrid approach, based on reputation score is recommended (Li, 2017).

Table I: Contributions and Limitations of Related Work

Ontology Graph (Ramaki, 2012)	Java, MATLAB	Drop of system overload rate, during computations	Dataset size is small
Text Analytics Processing (Sahri, 2018)	Protege, RapidMiner	Knowledge representation of financial criminology domain has been presented	There is no SWRL rule in ontology for fraud detection, cannot detect fraudulent transactions
Topic Modeling (Attigeri, 2018)	Wordnet, Protege, Python	Knowledge base ontology for digital fraud detection has been formulated	Dataset size is small
Ontology Based on Electronic Payment Fraud Prevention (El Orche, 2018)	Protege	Ontology-based approach for fraud prevention has been proposed	Experiment results are not reported.
Decision Tree (Save, 2017)	Not reported	System detects the fraudulent transaction at the time of transaction	Testing and implementation of results are not reported
Artificial Neural Network (Omar, 2017)	MATLAB	Achieve high predictive level to predict financial criminal reporting	Dependent on the interconnection between the neurons
Artificial Immune Systems (Halvaiee, 2014)	Hadoop, MapReduce	Increase accuracy, reduce the cost and response time	Memory cell generation is time consuming

Whale Algorithm Optimized BP Neural Network (Wang, 2018)	MATLAB	Credit card fraud detection accuracy is high and convergence speed is fast	Data set is very unbalanced
Feature Selection and Evolutionary Algorithms (Pouramirarsalani, 2017)	MATLAB	Combining the strengths of feature selection and genetic algorithm, proposed a system for fraud detection in e-banking	Dataset size is small
Support Vector Machine and Artificial Neural Network (Chen, 2005)	SmartNeuron 0.42	Study shows that both support vector machines and backpropagation networks can have well tested accuracy	Prediction accuracy depends on contradiction ratio
Hybrid methodology for credit card anomaly detection (Jadvani, 2018)	Results Not Reported (NR)	Comparison of different algorithms has been presented	Experiment results are not reported
Support Vector Machine and Decision Tree (Nipane, 2016)	LIBSVM	Three levels based fraudulent detection system has been proposed	Results are not comprehensive
Hidden Markov Model and Genetic Algorithm (Gaur, 2017)	SQL	System's performance is enhanced in terms of precision, recall, F-measure	Results are not comprehensive
Hash Based Technique using Data Mining (Pooja, 2018)	Results not reported	Money laundering detection model has been proposed	Results NR

Though reputation score is not available always, so it can be calculated by careful modeling of edge potential and tuning the parameters in markov random field. Social Network Analysis (SNA) reveals very useful information regarding groups, group activities and interaction among actors. Similarly, the analysis of online social networks is being carried out to detect financial frauds. Zhou et al. (2017) proposed a ProGuard technique to detect malicious accounts and account activities. SNA investigates social structures through networks and characterizes structures in terms of individual nodes and relationships between nodes within the network. Using SNA, authors proposed a solution to the problem of money laundering (Colladon, 2017; Hamid, 2017; Shaikh, 2018). Ontology is the best way to represent knowledge in a dynamic environment.

An ontology graph-based credit card fraud detection system is proposed by Ramaki et al. (2012). del Mar Roldan-Garcia et al. (2017) proposed an ontology-driven approach for examining and finding inconsistencies, mistakes and contradictions in Semantic Web Rule Language (SWRL) rules for fraud prevention. Furthermore, a lot of techniques are used for fraud detection in financial institutes. Machine learning is an application of AI that provides the ability to automatically learn. However, researchers have proposed different approaches for fraudulent transaction detection using supervised machine learning and supervised machine learning methods. Snchez et al. (2009) proposed the Association Rule (AR) based methodology for CC fraud detection. This approach is applied to the data of retail companies in Chile.

A hybrid method using AR and process mining has been proposed (Sarno, 2015) to solve the problem of fraud detection. In this work, authors developed rules (positive and negative) using the itemset of AR learning. Moreover, approaches based on KNN and outlier detection have been analyzed and implemented by Malini et al. (2017) to optimize the best solution for the CC fraud detection problem. Performance analysis of the results of various approaches used for CC fraud detection has been presented by MishraA et al. (2017). In addition to the comparative study, authors also proposed a model based on Artificial Neural Networks (ANN) for CC fraud detection (MishraA et al., 2017). Classification model has been developed (Sahin, 2011) using ANN and logistic regression to solve the problem of CC fraud detection. The model has been tested on the real dataset. Xuan et al. (2018) proposed Random Forest (RF) learning method for the fraud detection problem. Two kinds of RF are used to train the pattern of suspicious and non-suspicious transactions. Experiments are conducted using data of e-commerce in

China. Halvaiee et al. (2014) proposed a nature inspired based, Artificial Immune System (AIS) technique for suspicious credit card detection. Using AIS, authors proposed a CC fraud detection system with increasing accuracy as well as decreasing the system cost and response time. Furthermore, the contributions and limitations of the literature review are shown in Table I.

However, considering limitations of the aforementioned works we proposed improved, extra featured and comprehensive ontology for financial fraud deterrence. We created Jena rules for fraudulent transaction detection. We also proposed an intimation rule-based alert generation algorithm for generating alerts. Finally, the results of the proposed model are compared with ontology-based and non-ontology based methods. Comparison results show that our proposed model outperforms the existing models.

3. Types of Fraud

There are variety of frauds that may be committed. The most common types of financial fraud are bank fraud, corporate fraud and insurance fraud (West, 2016). However, our focus in this research work is on bank fraud. Bank fraud could be of any type. The brief description of common types of bank fraud is listed below. Further categorization of financial fraud is shown in Fig. 1. Moreover, Fig. 3 shows the timeline of different types of financial fraud detection methods reviewed in this paper.

3.1. Credit Card Fraud

CC fraud can be defined as unauthorized use of CC account to perform illegal transactions (through a wide variety of methods) from the compromised CC account. The purpose of an illegal transaction may be to purchase services without paying. This type of fraud can be performed using either a stolen physical card or payment card (credit card/debit card). Development of an accurate system for CC fraud detection is a critical problem. Recently, numerous fraud detection techniques have been proposed by research community for CC fraud detection. Behera et al. (2015) proposed a threelayered system for CC fraud detection using fuzzy clustering and neural network. The system performs verification of card details in the first phase. It calculates suspicious scores using fuzzy c means in the second phase.

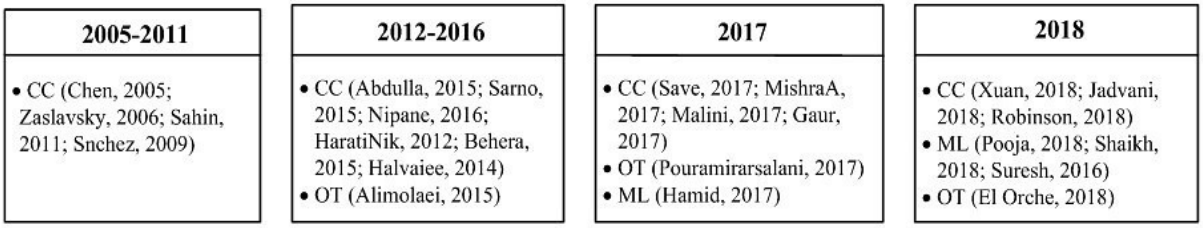

Fig. 3: Timeline of Financial Fraud Detection Methods

Finally, the third phase performs model has been tested on the real dataset. Xuan et al. (2018) proposed Random Forest (RF) learning method for the fraud detection problem. Two kinds of RF are used to train the pattern of suspicious and non-suspicious transactions. Experiments are suspicious activity detection.

3.2. Money Laundering

A process of hiding the source of illegitimately obtained cash (money) is known as Money Laundering (ML). ML fraud can be performed via illegal businesses. The basic reason for fraud is to get financial benefit in any form or shape like money. ML detection is still a critical challenge. However, a lot of ML detection systems and techniques have been analyzed and practiced in recent years. Hybrid of data mining-based Hash Based Association

(HBA) and Graph Theoretic (GT) method is used (Suresh, 2016; Pooja, 2018) for ML detection. This method identifies the traversal path of the Laundered money using HBA approach. Moreover, it detects the agent of ML by using the GT Approach. Carnaz et al. (2017) proposed an ontology-based framework. Furthermore, this framework is implemented in the use case of ML.

3.3. Online Transaction Fraud

Online transaction (also known as a PIN-debit transaction) is a process of transferring money or funds online. Electronic banking or Online Transaction (OT) fraud is an illegitimate transaction, which can happen via the internet. In a payment system, there are five entities (cardholder, merchant, card issuer, acquirer and payment corporation network) that are involved during payment transaction (El Orche, 2018). Payment process comprises of seven steps as shown in Fig. 4.

OT fraud detection continues to become a bigger issue. However, research is going on to detect OT frauds in financial institutes since long. Moreover, the timeline of (CC, ML and OT) fraud detection techniques (reviewed in this paper) are presented in Table II.

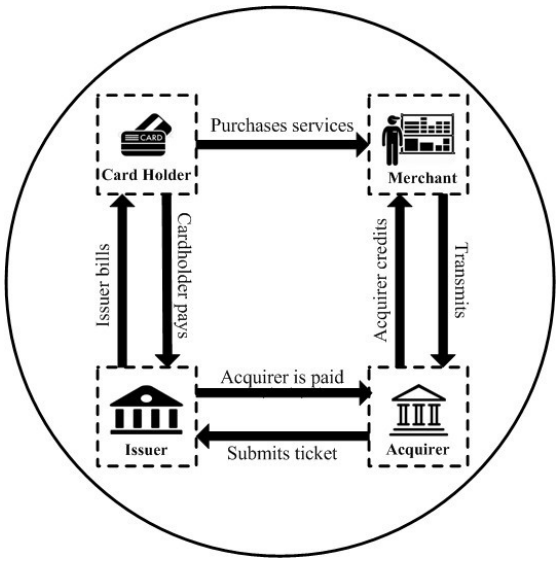

Fig. 4: Payment Process

4. System Model and Problem Formulation

In this section, we have discussed the explanation of system working and problem formulation in detail.

Table II: Timeline of FFD Techniques

Year	Type	Techniques
2005	CC	Support Vector Machine and Artificial Neural Networks (Chen, 2005)
2006	CC	Self-Organizing Map (Zaslavsky, 2006)
2007	CC	K-Nearest Neighbor and Outlier Detection (Malini, 2017)
2011	CC	Logistic Regression and ANN (Sahin, 2011)
2012	CC	Fuzzy (HaratiNik, 2012)
2014	CC	Artificial Immune Systems (Halvaiee, 2014)
2015	CC	Fuzzy Clustering and NN (Behera, 2015) Association Rule Learning and Process Mining (Sarno, 2015) Support Vector Machines and GA (Abdulla, 2015)
2015	OT	Fuzzy (Alimolaei, 2015)
2016	CC	Support Vector Machine and Decision Tree (Nipane, 2016)
2017	ML	Social Network Analysis (Hamid, 2017)
2017	OT	Genetic Algorithm and Feature Selection (Pouramirarsalani, 2017)
2017	CC	Decision Tree (Save, 2017) Artificial Neural Networks (MishraA, 2017) Hidden Markov Model and Genetic Algorithm (Gaur, 2017)
2018	CC	Hidden Markov Model and Fuzzy Logic (Jadvani, 2018) Hidden Markov Model (Robinson, 2018) Random Forest (Xuan, 2018) Random Forest and KNN (Nami, 2018) Whale Swarm Optimization Algorithm (Wang, 2018)
2018	ML	Hash Based Association and Graph Theoretic (Suresh, 2016) Random Forest and KNN (Nami, 2018) Hash Based (Pooja, 2018) Social Network Functions (Shaikh, 2018)
2018	OT	Ontology Based Fraud Prevention (El Orche, 2018)

4.1. System Description

In this section, the explanation of an enhanced financial fraud detection system is presented. We developed an ontology-based alert model with extra features. Extra features (in terms of defining severity level criteria using intimation rules) have been added to the proposed model. The result shows the significantly improved performance of our system. The overall functionality of the system is shown in Fig. 6. The proposed IRB alert generation algorithm is shown in Algorithm 1. However, explanation of system working (stepby-step execution) of the proposed system as shown below:

- Data from external data source e.g. relational database will be preprocessed and saved in the ontological database.
- Account transaction thresholds will be calculated after the data is updated in the ontological database. Thresholds will be calculated for each account and

these will be utilized by the inference engine during rules evaluation against each account transactions. Instead of using fixed thresholds, these thresholds will make the system more effective for fraud detection by keeping in view the transaction behavior of the customer.

Moreover, with the help of threshold, the system will adaptively tune itself with the changing behavior of the customer over the passage of time. Another important step

i.e. initial feedback from the customer about its

Algorithm 1 IRB Alert Generation Algorithm

```
Input Data:- Original Data, Inferred Data, Alert Rules, Alert Generation Rules
Output:- Alert Notifications, Transaction-IRI, Transaction ID, Severity Level
Data entry in the ontological database
Data preprocessing and saving
for All data from relational a database to resource description framework store do
    Calculate account transaction thresholds
    Apply rules (executed by inference engine)
    if Indicate risks then
        Apply intimation-rule
        if Severity level -> high then
            Pass through severity levels
            of Intimation-Rules
            If fraud detected!!
            Generate alert notifications
        end if
        Return Transaction-IRI
        Return Transaction-ID
        Return Severity Level
    end if
end for
```

transactional behavior can be added in the system to evaluate real-time transactional behavior. For example, a customer may fill the form telling that what is expected average withdrawal amount per month.

- These rules will define the criteria that how to set the severity level of the alert generated. For example, If the inferred transaction's withdrawal amount >= 2 * withdrawal-avg-monthly, then the severity level of the alert generated must be higher than normal.
- Inferred transactions are inference engine generated transactions resulted in the execution of Jena rules on available data. Alerts will be generated (using intimation-rules) with a certain severity level. The system will treat alerts with three severity levels using intimation-rules.

•

i. Level 1: Suspected alert, when the first occurrence identified (Severity Level: Low).

ii. Level 2: Investigation Required (Severity Level: Medium).

iii. Level 3: Fraud Detected (Severity Level: High). This severity level can be used by fraud notification module to take necessary action like generating email or SMS etc.

- Additionally, intimation-rules could be defined to cater to special cases (festivals and events) like for new year event, withdrawal amount can be two times the average monthly withdrawals. Suppose, there are two cases, E and M. Where E is special event in month M. Other than month M, if the withdrawal amount is greater than the average monthly withdrawal amount, it may be treated as fraud but for special event E its severity level will be lower as it is expected to have higher withdrawals on this event. An example of intimation rule for withdrawals in month M is shown below.

*Rule19 :SumOfWithdrawal(w30AMT) as Withdrawals, Account(hasConAcc) as Consumer Account from Account as join Account as Join Person as Customer = hasConAcc and transaction TimeStamp during and Transaction Month (M), where month as 30 days and Event (E) days = 3, hasAvgDep(avgWithdrawal) and transaction Type=Withdrawal having Withdrawals > (Withdrawal-Avg-Monthly * 2) as 2XavgWithdrawal*

Corresponding Jena syntax of intimation rule is presented in Table IV. Furthermore, Fig. 5 shows an example that lists all transaction that satisfies the aforementioned rule. • If the same type of alert is previously generated for the same customer account, then the system may increase the hit count and change the severity level.

- The web interface will help in monitoring these alerts and the administrator may mark some alerts dead with additional notes explaining the reason. These dead alerts

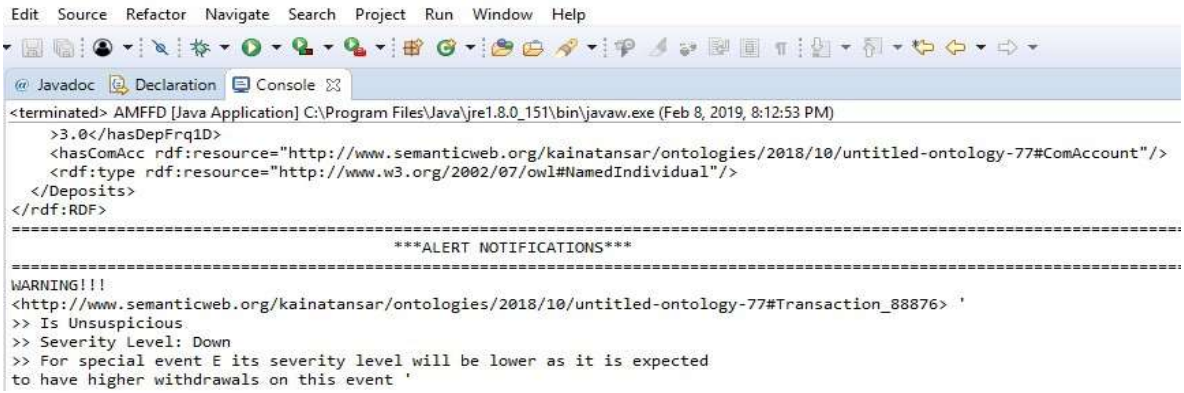

Fig. 5: Alerts Generated

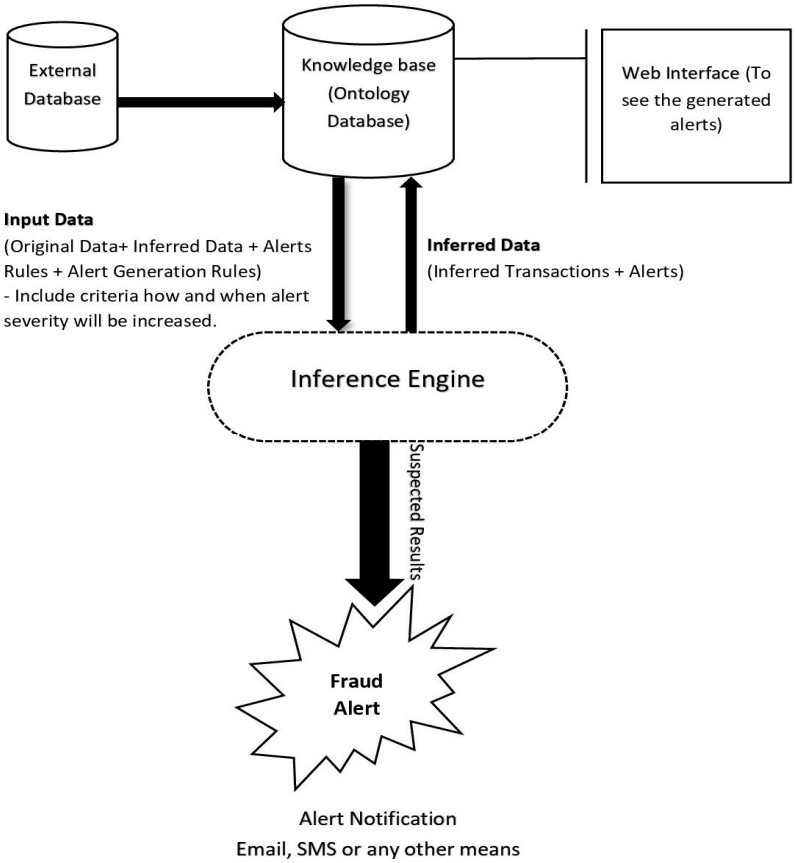

Fig. 6: Overall System Working

will be excluded from future inferencing for performance improvement. Administrator will mark the alerts dead after an action has been taken against them.

1.1 4.2. Problem Formulation

We formulate the problem of financial fraud detection as a single-objective optimization problem. Suppose, there are two transactions T_{cml} and T_{cnr}.

$$T_{cml,} = (T_{cml,1}, T_{cml,2}, T_{cml,3}, .., T_{cml,m}) \quad (1)$$

$$T_{cnr,} = (T_{cnr,1}, T_{cnr,2}, T_{cnr,3}, .., T_{cnr,n}) \quad (2)$$

Where, T_{cml} are transactions from commercial account and T_{cnr} are transactions from consumer account.

$$T = T_{cml} + T_{cnr} \quad (3)$$

Manuscript received June 5, 2025
Manuscript revised June 20, 2025
https://doi.org/10.22937/IJCSNS.2025.25.6.19

In transactions T, fraudulent F and legitimate L transactions are the subset of transaction T, ($F \subset T, L \subset T$). Whereas, in sets F and L number of transactions varying from 1 to m and latter from 1 to n.

$$F = (F_1, F_2, F_3, .., F_m) \quad (4)$$

$$L = (L_1, L_2, L_3, .., L_n) \quad (5)$$

$$T = F \cup L \quad (6)$$

Transaction is either legitimate or fraudulent, as status shown in equation (7)

$$\alpha_{ij} = \begin{cases} 1, & \text{is fraudulent,} \\ 0, & \text{is legitimate.} \end{cases} \quad (7)$$

The objective is to minimize fall-out and miss rate as shown in the below equation.

$$Minimize \sum_{i=1}^{n} \sum_{j=1}^{m} FN_{ij} + FP_{ij} * \alpha_{ij} \quad (8)$$

Where FN is the number of objects of set F, which were expected as an object of L incorrectly. FP is the number of objects of set L, which were expected as an object of F incorrectly. FP is also known as the fall-out rate.

5. Ontology Contruction Methodology

In this work, METHONTOLOGY (Corcho, 2005) is used to illustrate the construction of ontology. This framework allows ontology modeling by means of graphical representations that can be perceived by a specialist in one domain who are not involved in the domain of ontology. METHONTOLOGY has several phases of the life cycle. It also identifies management and support activities (Corcho, 2005). Management activities, which includes control, quality assurance and schedule. Support activities, such as configuration management, documentation, evaluation, integration and knowledge acquisition, while development activities are specification, conceptualization, formalization, implementation and maintenance, as shown in Fig. 7.

5.1. Formal Representation of FFD Ontology

The ontology represents knowledge in a dynamic environment by making the knowledge easily shareable and reusable. It describes the terms and their relationships of the given domain. Structure of an ontology consists of concept identifiers, relation identifiers, attribute identifiers and data types (Cimiano, 2006). Moreover, the structure of ontology can be represented as:

$$O = Ontology = (C, \leq_t, S, P, I, R) \quad (9)$$

Where C is the set of classes, $\leq_t$ on C is called concept hierarchy. S stands for subclasses, P represents object and data properties. I represents a set of individuals and rules are represented by R. Moreover, they can be represented as follows:

$$C = \left(\prod_{i=1}^{n} C_i, \leq_t \right) \quad (10)$$

Where i = (1,2,3,...,n) and ≤ fulfills the conditions (Cimiano, 2006) as shown below.

$$\forall a, (a \leq a) \quad (11)$$

$$\forall a \, \forall b, (a \leq b \wedge b \leq a \Rightarrow a = b) \quad (12)$$

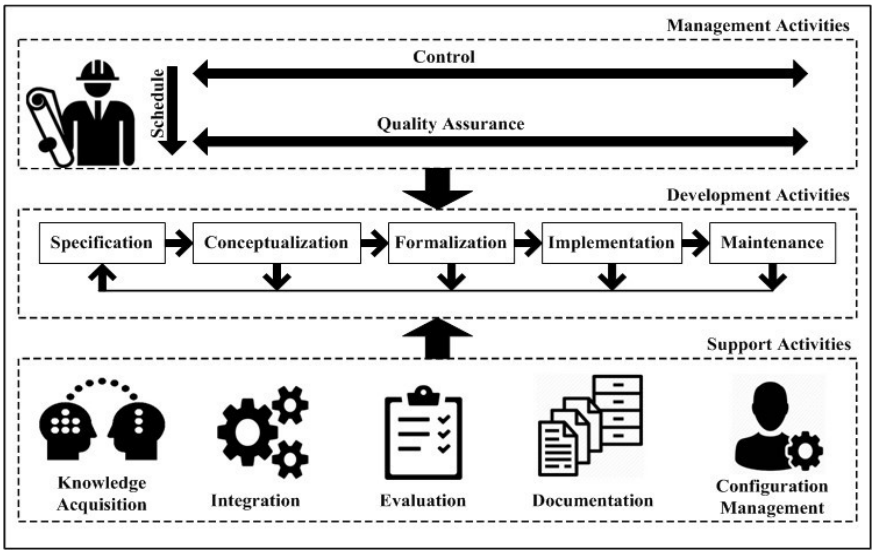

Fig. 7: Ontology Construction Activities Proposed by METHONTOLOGY

$$\forall a\ \forall b\ \forall c,\ (a \leq b \wedge b \leq c \Longrightarrow a \leq c) \quad (13)$$

$$\forall a\ (a \leq top\ element) \quad (14)$$

Furthermore, each property has relationships with the class associated with domain and range. Fig. 8 shows the object properties, data properties and instances of our proposed FFD ontology model.

6. FFD Ontology Implementation

This section presents the proposed FFD model. In this work, an ontology-based expert system along with rules has been introduced to detect suspicious transactions. The system is composed of three main components:

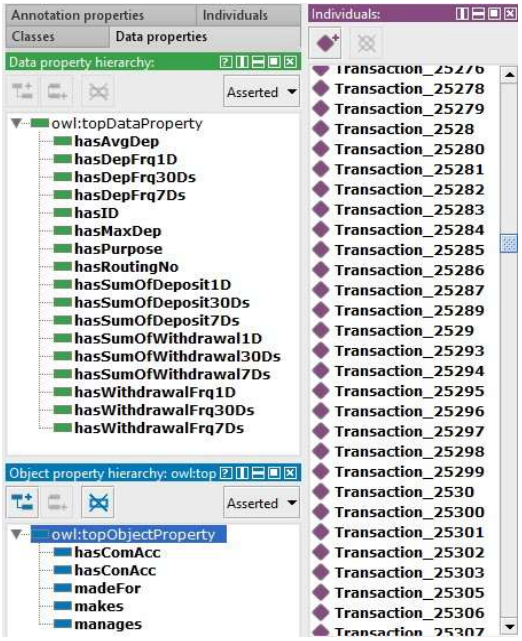

Fig. 8: Properties and Instances of FFD Ontology

- Ontology Development
- Ontology Reasoning
- Results by Querying on Inferred Ontology

6.1. Ontology Development

Ontology development starts with the data preprocessing step in which specific data items will be selected, which will later be transformed into an ontology. During this process, all the irrelevant and redundant information will be filtered out for making data more meaningful. A step-by-step ontology development process is depicted in Fig. 9. For dataset normalization, data preprocessing is an important phase in the ontology development process.

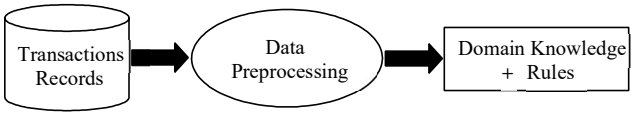

Fig. 9: Ontology Development

Table III: Rules for Fraudulent Transaction Detection

Rule #	Description
For Commercial Accounts	
1	Repeated deposits of cash in a week (greater than TA1).
2	Repeated withdrawals in a week (exceed limit TA1).
3	More than two instances in a week where customer makes two or more deposits on the same day (total deposit is greater than TA2).
4	Over TA1 deposit and greater than 25% of customer's highest cash deposit.
5	Over TA2 deposit and 150% of customer's average cash deposit.
6	Cash withdrawal (more than TA3), made for payroll.
7	Traveler's cheque deposits, more than TA4.
8	Money order deposits, more than TA4.
9	Purchase of Certificate of Deposit (CD) with cash (more than TA3).
10	Over TA3 deposit in a week, made from wire transfer.
11	More than two instances in a week, where large bills (exceed limit TA3).
12	More than two instances in a week, where small bills (exceed limit TA4).
For Consumer Accounts	
13	More than two deposits in a week (total deposit is greater than TA3).
14	More than two deposits in a month (total deposit is greater than TA1).
15	More than one withdrawal in a month (total amount greater than TA3).
16	Purchase with cash of CD for greater than TA4.
17	Over TA4 deposits in a day made for money order.
18	Over TA4 deposits in a day, made in travelers's cheque.
19	Cater to special cases (festivals and events), the withdrawal amount can be two times the average monthly withdrawals.

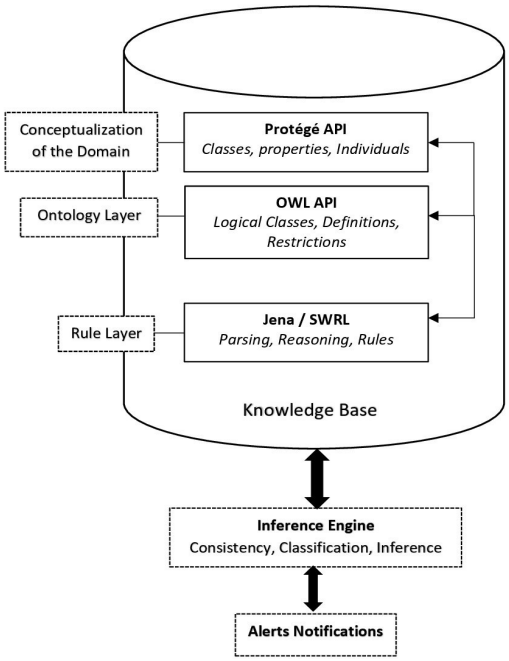

Fig. 10: High-Level System Architecture Diagram

The system consists of the domain knowledge (transactions data) modeled using ontology and defining rules on the top to support reasoning. Based on these rules inference engine will infer new knowledge which will be used to identify suspicious transactions. However, the knowledge base of our proposed ontology model consists of a collection of customers transactions data. The ontology model consists of classes, subclasses, object and datatype properties and instances. These records include transaction amount and their frequency in a given time interval etc. The following three layers of ontology design are residing in the knowledge base. However, the threelayered high-level system architecture is depicted in Fig. 10.

i. Conceptualization of the domain Layer:In this layer, the customer's transactions are modeled in the form of classes, subclasses, properties (object and data type) and instances. The main classes of our alert ontology model are account, person, purposes, suspicious-alerts and transaction-type, as depicted in Fig. 14.

ii. Ontology Layer:

The ontological layer defines restrictions upon classes by using Ontology Web Language (OWL) and facilitates logic. Furthermore, the hierarchy of the proposed ontology model (classes and subclasses), a graphical representation of FFD ontology is shown in Fig. 14.

iii. Rule Layer:

To infer new knowledge out of the existing knowledge, rules are developed on top of the ontology OWL layer. In this study, the rules are presented in Jena. Jena is a semantic web toolkit (Carroll, 2004). It is a Java framework for the creation of applications for the Semantic Web. There are three levels of rules (as discussed previously) executed by the inference engine. To identify the fraudulent transaction, rules are created using the Anti Money Laundering (AML) guidelines provided by the financial regulatory authority. The AML policy guidelines (set of rules) are shown in Table III. Furthermore, Table IV shows the corresponding Jena syntax. It should be mentioned that the values of Threshold Amount (TA) are not fixed. These threshold values may vary depending on the AML guidelines used in different countries. However, in this work, we have suggested these values as TA1 is equal to 10000 USD, TA2 is 8000 USD, TA3 is 5000 USD and TA4 is equal to 3000 USD.

6.2. Ontology Reasoning

Once the ontology is developed and populated with transactions records along with the rules, reasoner will be able to infer logical consequences from the set of asserted facts (inferring new knowledge from the knowledge base). The inference rules are commonly specified by means of an ontology language. Traditional reasoning engine (Pellet, HermiT, FaCT++ etc.) can be used for reasoning (Khamparia, 2017). However, we have used the FaCT++ 1.6.5 reasoning engine in this work. Furthermore, a general reasoning model is shown in Fig. 11.

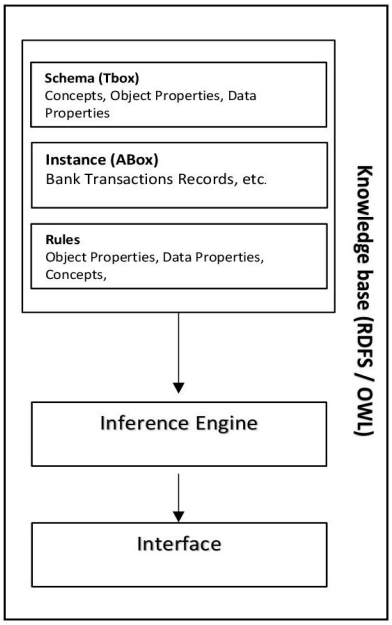

Fig. 11: Ontology Reasoning

6.3. Results by Querying on Inferred Ontology

Once the inference engine generates inferred results based on the rules, then stored transactions knowledge can be queried (using query language) to obtain the required information.

SPARQL is the standard query language (Sirin, 2007). In this work, we have used SPARQL to query the FFD ontology. Results of the SPARQL query are presented in Fig. 12. Query lists all the classes and its corresponding subclasses of FFD ontology.

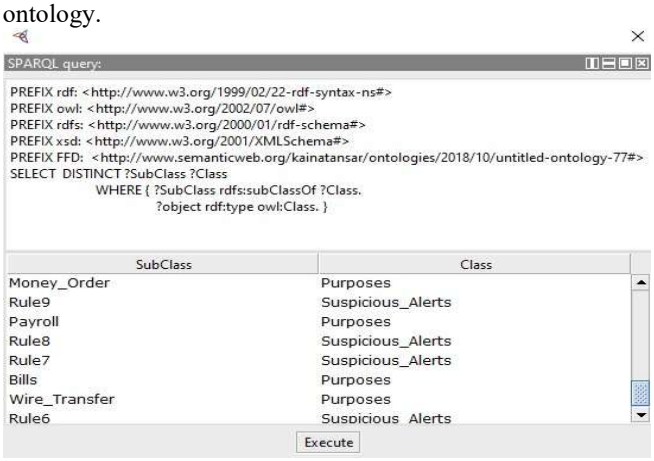

Fig. 12: Result of SPARQL Query

7. Ontology Validation

In this section, we have discussed the methodology, constraints and assumptions of FFD ontology validation.

7.1. OntoClean Methodology

In this work, we have used OntoClean (Guarino, 2004) for ontology validation. It is a formal methodology for evaluating the ontological sufficiency of taxonomic relationships. Property of a property is known as meta-property. Unity, identity, rigidity, dependency and essence are meta properties (formal notions) of OntoClean. Meta property can be further classified into three main labels (+, -, ~). Description of each label is shown in Table V. Furthermore, these formal notions are used to characterize relevant aspects of the intended meaning of the properties, classes and relations in an ontology. According to the aforementioned notions, OntolClean attaches the meta properties to each concept and removes false relationships. Ontology Works designed a system that automatically checks the reliability and removes incorrect relationships in ontologies after defining the meta-properties (notions). OntoClean provides a formal and straightforward approach to explain the most common inconsistencies in the ontological model. It further checks the consistency, conciseness and completeness of ontology. However, in this work, we have used the OntoClean method for validation of FFD ontology. Validation criteria of OntoClean method are shown below.

7.2. Constraints and Assumptions

For validating and ensuring the accuracy of ontology, conditions are applied to classes and properties (Guarino, 2004). Assume, there are two properties, X and Y, when Y subsumes X, so their resulting restrictions hold as follows:

1) If Y has anti-rigid (~R), then X must have anti-rigid (~R).
2) A ~R property cannot subsume a +R property. 3) If Y is rigid (+R), then X must be rigid (+R).
4) A +R property cannot subsume a ~R property.

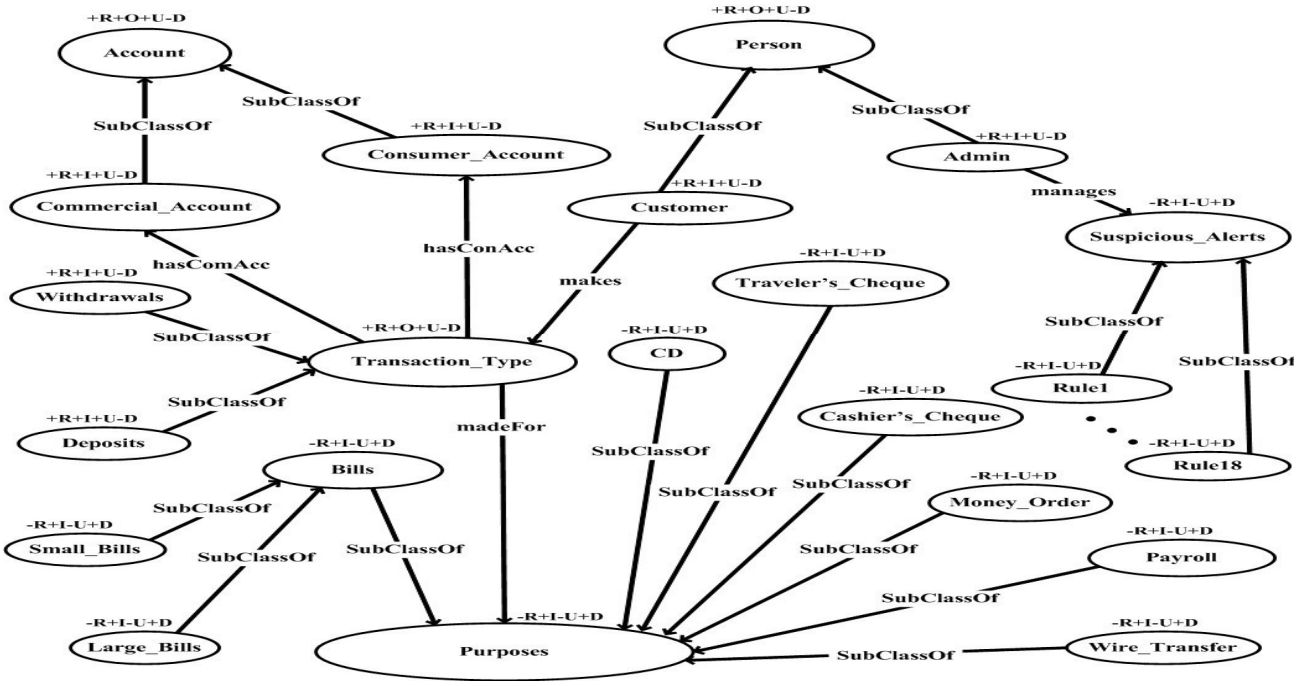

Fig. 13: FFD Ontology Va;lidation Through OntoClean

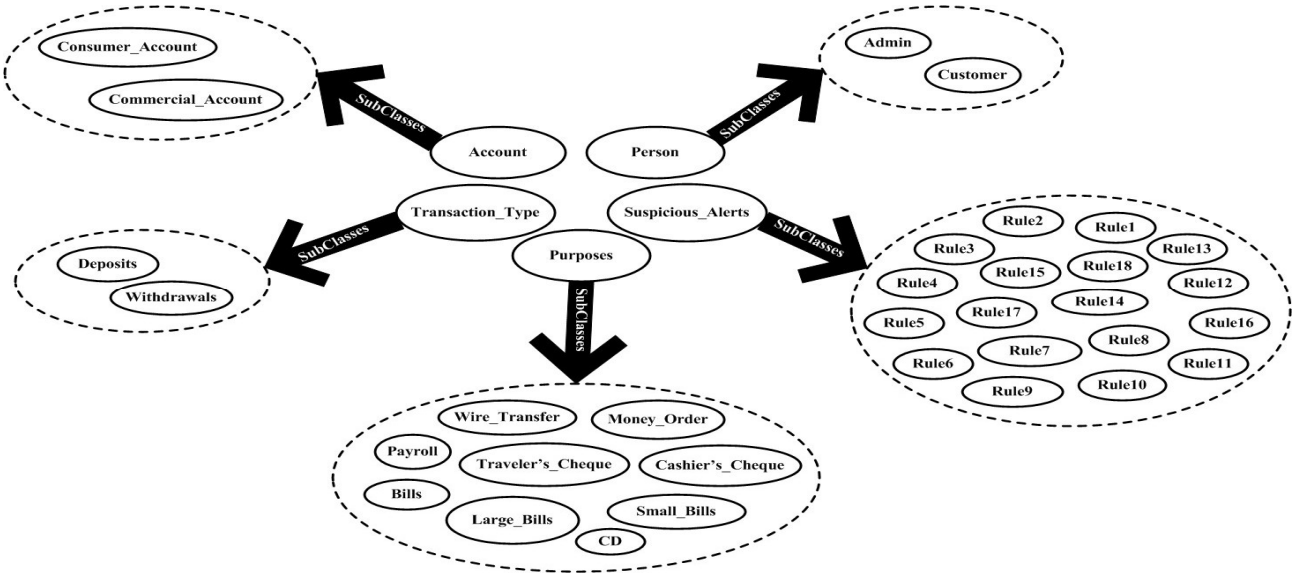

Fig. 14: Graphical Representation of FFD ontology

8. Simulation Setup and Results

8.1. Dataset

In this section, we have discussed the dataset, simulation For experiments, we have used real dataset. The dataset tools, measures and comparison of results in detail. contained 1048576 individual transactions. In the dataset, transactions are integrated into days, weeks and months. The most important features in the dataset are the total deposit and withdrawal amount, the frequency of deposit, and frequency of withdrawal in days, weeks and months respectively. The transaction record is separated by deposits and withdrawal to capture the flow of money.

8.2. Simulation Tools

The experiments were conducted on a Windows 10 with 4Gb RAM, 1.70 GHz Intel Core i3. In this work, we have used simple tools for compiling results. These tools are listed below:

1. Eclipse IDE
2. Java
3. Protege 5.2.0 Ontology Editor
4. SPARQL query language
5. Apache Jena 3.9.0 Semantic Web Framework
6. FaCT++ 1.6.5 Reasoner

We have used Eclipse IDE for editing the code. Java is used for executing Java code. We use Protege 5.2.0 to develop FFD ontology and SPARQL query language to query the financial fraud detection ontology. Moreover, we have used apache Jena for manipulating ontologies and rules construction purpose, while FaCT++ 1.6.5 is used to infer new knowledge from the knowledge base. Following on, we discuss the experimental results of FFD in detail.

Table V: Description of Meta Properties

Meta Property	Description
+R (Rigid)	All object must be objects of this concept in every possible world.
-R (Non-Rigid)	Objects will stop being objects of the concept.
~R (Anti-Rigid)	objects will not any longer be the object of that concept.
+I (Identity)	Objects carry unique identification criteria from any parent class.
-I (Non-Identity)	There are no identification criteria.
+O (Supply Iden-tity)	Objects themselves provide a unique identification criteria.
+U (Unity)	Objects are ”whole” and have a single unit criteria.
-U (Non-Unity)	Objects are ”whole” and do not have a single unit criteria.
~U (Anti-Unity)	Objects are not ”whole”.
+D (Dependence)	Dependency exists.
-D (Non-Dependence)	No dependency.

8.3. Evaluation Measures

Before we describe the experimental results, we first introduce the metrics. In this work, the metrics we used for performance comparison of the FFD system are accuracy, precision, recall, F-measure and Matthews Correlation

Coefficient (MCC). Furthermore, the formulas of the aforementioned measures are presented below:

$$Accuracy = \frac{TP + TN}{TP + FP + TN + FN} \quad (15)$$

$$Precision = \frac{TP}{(TP + FP)} \quad (16)$$

$$Recall = \frac{TP}{(TP + FN)} \quad (17)$$

$$F - measure = \frac{2 * Precision * Recall}{Precision + Recall} \quad (18)$$

$$MCC = \frac{TP * TN - FP * FN}{\sqrt{(TP + FP)(TP + FN)(TN + FP)(TN + FN}} \quad (19)$$

Where,

- TP = Number of Legitimate Transactions (LTs) which were identified correctly.
- FN = Number of LTs which were expected as Fraudulent Transactions (FTs) incorrectly.
- TN = Number of FTs which were identified correctly.
- FP = Number of FTs which were expectedas LTs incorrectly.

8.4. Results and Performance Comparison

Our proposed ontology-based (extra featured) system generates alerts at the onset of suspicious activity. Alerts will be generated with three severity level (as discussed previously in section 4). Alert notifications generated by the FFD system are shown in Fig. 15. The results of the proposed FFD ontology-based system are compared with ontology-based and non-ontology based techniques. Table VI shows comparative analysis (in terms of classes, subclasses, properties, rules and precision) of the proposed FFD with ontology-based techniques. In Table VII, the performance results of the proposed FFD system are shown.

Table VI: Comparison with Ontology-Based Systems

Reference	Classes + SubClasses	Properties	Rules	Precision
Ramaki et al. (2012)	23	NR	NR	89.4%
Sahri et al. (2018)	9	2	NR	NR
Rajput et al. (2014)	19	10	7	NR
Attigeri et al. (2018)	8	2	NR	NR
ElOrche et al. (2018)	5	6	3	NR
Proposed FFD	40	22	19	92.3%

TABLE VII: Performance of the Proposed System

Measure	Accuracy	Precision	Recall	F-measure	MCC
Value	99%	92.3%	80%	85.7%	0.8592

For performance comparison of our proposed FFD system with non-ontology based techniques, metrics we used are accuracy, precision, recall and F-measure. However, performance comparison results of the proposed FFD with non-ontology based (RF-I and RF-II) techniques (Xuan, 2018) are shown in Fig. 16. The result shows that the accuracy and precision of the FFD system are increasing, while the F-measure is decreasing as compared to RF-II. However, the recall gets the maximum value as compare to RF-I. Furthermore, the results show that our proposed system outperforms the existing systems.

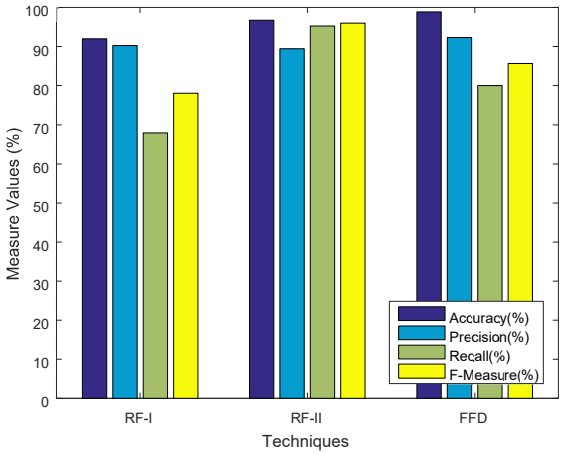

Fig. 16: Comparison with Non-Ontology Based Techniques

9. Conclusions and Future Works

This article has introduced fraud trends in financial institutes. We described data representational models and the advantages of using ontologies over databases. We proposed an ontology-based FFD system (with additional features) for fraud deterrence. We also proposed an IRB alert generation algorithm for alert generation. One strength of our ontologybased alert model is its ability to reason. Reasoning capability in ontologies makes it possible to derive facts (that are not described in the knowledge base clearly). Furthermore, from inferred transactions, this system has introduced alert severity level and dead alerts exclusion mechanism as described in the aforementioned section. This additional feature makes our system faster and

more efficient. We hope this article can encourage more research efforts towards the realization of fraud deterrence in any technological system that involves money and services.

In future, we will investigate the performance of our proposed FFD system in other fraud areas. Furthermore, fraud case studies in other domain (telecommunication, internet marketing and insurance fraud) will extremely desirable to test the performance of same technique.

References

[1] Abdallah, A., Maarof, M. A., & Zainal, A. (2016). Fraud detection system: A survey. Journal of Network and Computer Applications, 68, 90-113.

[2] Abdulla, N., Rakendu, R., & Varghese, S. M. (2015). A Hybrid Approach to Detect Credit Card Fraud. International Journal of Scientific and Research Publications, 5(11).

[3] Alimolaei, S. (2015, September). An intelligent system for user behavior detection in Internet Banking. In 2015 4th Iranian Joint Congress on Fuzzy and Intelligent Systems (CFIS) (pp. 1-5). IEEE.

[4] Attigeri, G., MM, M. P., Pai, R. M., & Kulkarni, R. (2018). Knowledge Base Ontology Building For Fraud Detection Using Topic Modeling. Procedia Computer Science, 135, 369-376.

[5] Behera, T. K., & Panigrahi, S. (2015, May). Credit card fraud detection: a hybrid approach using fuzzy clustering & neural network. In 2015 Second International Conference on Advances in Computing and Communication Engineering (pp. 494-499). IEEE.

[6] Carnaz, G., Nogueira, V., & Antunes, M. (2017). Ontology-Based Framework Applied to Money Laundering Investigations.

[7] Carroll, J. J., Dickinson, I., Dollin, C., Reynolds, D., Seaborne, A., & Wilkinson, K. (2004, May). Jena: implementing the semantic web recommendations. In Proceedings of the 13th international World Wide Web conference on Alternate track papers & posters (pp. 74-83). ACM.

[8] Chen, R. C., Luo, S. T., Liang, X., & Lee, V. C. (2005, October). Personalized approach based on SVM and ANN for detecting credit card fraud. In 2005 International Conference on Neural Networks and Brain (Vol. 2, pp. 810-815). IEEE.

[9] Cimiano, Philipp. Ontologies. Springer US, 2006.

[10] Colladon, A. F., & Remondi, E. (2017). Using social network analysis to prevent oney laundering. Expert Systems with Applications, 67, 49-58.

[11] Corcho, O., Fernndez-Lpez, M., Gmez-Prez, A., & Lpez-Cima, A. (2005). Building legal ontologies with METHONTOLOGY and WebODE. In Law and the semantic web (pp. 142-157). Springer, Berlin, Heidelberg.

[12] Dadjoo, M., & Kheirkhah, E. (2015). An approach for transforming of relational databases to OWL ontology. arXiv preprint arXiv:1502.05844. Dal, A. P., Boracchi, G., Caelen, O., Alippi, C., & Bontempi, G. (2018).

[13] Credit Card Fraud Detection: A Realistic Modeling and a Novel Learning Strategy. IEEE transactions on neural networks and learning systems, 29(8), 3784-3797. del Mar Roldan-Garcia, M., Garca-Nieto, J.,& Aldana-Montes, J. F. (2017). Enhancing semantic consistency in anti-fraud rule-based expert systems. Expert Systems with Applications, 90, 332 343.

[14] Delamaire, L., Abdou, H. A. H., & Pointon, J. (2009). Credit card fraud and detection techniques: a review. Banks and Bank systems, 4(2), 57-68.

[15] El Orche, A., Bahaj, M., & Alhayat, S. A. (2018, October). Ontology Based on Electronic Payment Fraud Prevention. In 2018 IEEE 5th International Congress on Information Science and Technology (CiSt) (pp. 143-148). IEEE.

[16] Furlan,., Vasilecas, O., & Bajec, M. (2011). Method for selection of motor insurance fraud management system components based on business performance: Transporto priemoni draudimo apgavysi valdymo sistemos komponent pasirinkimo metodas, grindiamas Verslo veiklos efektyvumu. Technological and economic development of economy, 17(3), 535-561.

[17] Ganji, V. R., & Mannem, S. N. P. (2012). Credit card fraud detection using anti-k nearest neighbor algorithm. International Journal on Computer Science and Engineering, 4(6), 1035 1039.

[18] Gaur, S., Maheshwari, A., Dhruwa, L., & Upadhyay, A. (2017). Hidden Markov Model and Genetic Algorithm Based Credit Card Fraud Detection.

[19] Guarino, N., & Welty, C. A. (2004). An overview of OntoClean. In Handbook on ontologies (pp. 151-171). Springer, Berlin, Heidelberg.

[20] Halvaiee, N. S., & Akbari, M. K. (2014). A novel model for credit card fraud detection using Artificial Immune Systems. Applied Soft Computing, 24, 40-49.

[21] Hamid, O. H. (2017, May). Breaking Through Opacity: A Context-Aware Data-Driven Conceptual Design for a Predictive Anti Money Laundering System. In 2017 9th IEEE-GCC Conference and Exhibition (GCCCE) (pp. 1-9). IEEE.

[22] HaratiNik, M. R., Akrami, M., Khadivi, S., & Shajari, M. (2012, November). FUZZGY: A hybrid model for credit card fraud detection. In 6th International Symposium on Telecommunications (IST) (pp. 1088-1093). IEEE.

[23] Jadvani, Rushabh, Vivek Parmar, Dhruvin Sangani, and Payal Sanghavi. Hybrid methodology for credit card anomaly detection. (2018).

[24] Khamparia, A., & Pandey, B. (2017). Comprehensive analysis of semantic web reasoners and tools: a survey. Education and Information Technologies, 22(6), 3121-3145.

[25] Lata, L. N., Koushika, I. A., & Hasan, S. S. (2015). A Comprehensive Survey of Fraud Detection Techniques. International Journal of Applied Information Systems, 10(2), 26-32.

[26] Li, Y., Sun, Y., & Contractor, N. (2017, July). Graph mining assisted semisupervised learning for fraudulent cash-out detection. In Proceedings of the 2017 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining 2017 (pp. 546-553). ACM.

[27] Makki, S., Haque, R., Taher, Y., Assaghir, Z., Ditzler, G., Hacid, M. S.,& Zeineddine, H. (2017, September). Fraud Analysis Approaches in the Age of Big Data-A Review of State of the Art. In 2017 IEEE 2nd International Workshops on Foundations and Applications of Self* Systems (FAS* W) (pp. 243-250). IEEE.

[28] Malini, N., & Pushpa, M. (2017, February). Analysis on credit card fraud identification techniques based on KNN and outlier detection. In 2017 Third International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB) (pp. 255-258). IEEE.
[29] Martinez-Cruz, C., Blanco, I. J., & Vila, M. A. (2012). Ontologies versus relational databases: are they so different? A comparison. Artificial Intelligence Review, 38(4), 271-290.
[30] MishraA, C., GuptaB, D. L., & SinghC, R. Credit Card Fraud Identification Using Artificial Neural Networks.
[31] Nami, S., & Shajari, M. (2018). Cost-sensitive payment card fraud detection based on dynamic random forest and k-nearest neighbors. Expert Systems with Applications, 110, 381-392.
[32] Nipane, V. B., Kalinge, P. S., Vidhate, D., War, K., & Deshpande, B. P. (2016). Fraudulent Detection in Credit Card System Using SVM & Decision Tree. International Journal of Scientific Development and Research (IDSDR), 1(5).
[33] Omar, N., Johari, Z. A., & Smith, M. (2017). Predicting fraudulent financial reporting using artificial neural network. Journal of Financial Crime, 24(2), 362-387.
[34] Patil, V., & Lilhore, U. K. (2018). A Survey on Different Data Mining & Machine Learning Methods for Credit Card Fraud Detection.
[35] Pooja, N. S., N. Shubha, K. H. Surabhi, G. K. Thejasvi, and J. Chandrika. Hash Based Technique for Detecting Suspicious Accounts in Money Laundering using Data Mining. (2018).
[36] Pouramirarsalani, A., Khalilian, M., & Nikravanshalmani, A. (2017). Fraud detection in E-banking by using the hybrid feature selection and evolutionary algorithms. IJCSNS, 17(8), 271 279.
[37] Quah, J. T., & Sriganesh, M. (2008). Real-time credit card fraud detection using computational intelligence. Expert systems with applications, 35(4), 1721-1732.
[38] Rajput, Q., Khan, N. S., Larik, A., & Haider, S. (2014). Ontology based expert-system for suspicious transactions detection. Computer and Information Science, 7(1), 103.
[39] 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.
[40] Robinson, W. N., & Aria, A. (2018). Sequential fraud detection for prepaid cards using hidden Markov model divergence. Expert Systems With Applications, 91, 235-251.
[41] Sahin, Y., & Duman, E. (2011, June). Detecting credit card fraud by ANN and logistic regression. In 2011 International Symposium on Innovations in Intelligent Systems and Applications (pp. 315-319). IEEE.
[42] Sahri, Z., Shuhidan, S. M., & Sanusi, Z. M. (2018). An Ontology-Based Representation of Financial Criminology Domain Using Text Analytics Processing. INTERNATIONAL JOURNAL OF COMPUTER SCIENCE AND NETWORK SECURITY, 18(2), 56-62.
[43] Sarno, R., Dewandono, R. D., Ahmad, T., Naufal, M. F., & Sinaga, F. (2015). Hybrid Association Rule Learning and Process Mining for Fraud Detection. IAENG International Journal of Computer Science, 42(2).
[44]]Save, P., Tiwarekar, P., Jain, K. N., & Mahyavanshi, N. (2017). A novel idea for credit card fraud detection using decision tree. International Journal of Computer Applications, 161(13).
[45] Sen, S. K., & Dash, S. (2013). Meta learning algorithms for credit card fraud detection. International Journal of Engineering Research and Development, 6(6), 16-20.
[46] Shaikh, A. K., & Nazir, A. (2018). A Model for Identifying Relationships of Suspicious Customers in Money Laundering using Social Network Functions. In Proceedings of the World Congress on Engineering (Vol. 1). Sirin, E., & Parsia, B. (2007, June). SPARQL-DL: SPARQL Query for OWL-DL. In OWLED (Vol. 258).
[47] Snchez, D., Vila, M. A., Cerda, L., & Serrano, J. M. (2009). Association rules applied to credit card fraud detection. Expert systems with applications, 36(2), 3630-3640.
[48] Suresh, C., Reddy, K. T., & Sweta, N. (2016). A hybrid approach for detecting suspicious accounts in money laundering using data mining techniques. International Journal of Information Technology and Computer Science (IJITCS), 8(5), 37.
[49] Wang, C., Wang, Y., Ye, Z., Yan, L., Cai, W., & Pan, S. (2018, August). Credit card fraud detection based on whale algorithm optimized bp neural network. In 2018 13th International Conference on Computer Science & Education (ICCSE) (pp. 1-4). IEEE.
[50] Wasilewska, A. Fraud Detection with AI.
[51] West, J., & Bhattacharya, M. (2016). Intelligent financial fraud detection: a comprehensive review. Computers & security, 57, 47-66.
[52] Xuan, S., Liu, G., Li, Z., Zheng, L., Wang, S., & Jiang, C. (2018, March). Random forest for credit card fraud detection. In 2018 IEEE 15th International Conference on Networking, Sensing and Control (ICNSC) (pp. 1-6). IEEE.
[53] Zanin, M., Romance, M., Moral, S., & Criado, R. (2018). Credit card fraud detection through parenclitic network analysis. Complexity, 2018.
[54] Zareapoor, M., & Yang, J. (2017). A novel strategy for mining highly imbalanced data in credit card transactions. Intelligent Automation & Soft Computing, 1-7.
[55] Zaslavsky, V., & Strizhak, A. (2006). Credit card fraud detection using self-organizing maps. Information and Security, 18, 48.
[56] Zhou, Y., Kim, D. W., Zhang, J., Liu, L., Jin, H., Jin, H., & Liu, T. (2017). Proguard: Detecting malicious accounts in social-network-based online promotions. IEEE Access, 5, 1990-1999.
[57] Zhou, X., Cheng, S., Zhu, M., Guo, C., Zhou, S., Xu, P., ... & Zhang, W. (2018). A state of the art survey of data mining-based fraud detection and credit scoring. In MATEC Web of Conferences (Vol. 189, p. 03002). EDP Sciences.