# *Business Process Anomaly Detection using Ontology-Based Process Modelling and Multi-Level Class Association Rule Learning*

Riyanarto Sarno
Department of Informatics
Institut Teknologi Sepuluh Nopember (ITS)
Surabaya, Indonesia
riyanarto@if.its.ac.id

Fernandes P. Sinaga
Department of Informatics
Institut Teknologi Sepuluh Nopember (ITS)
Surabaya, Indonesia
fernandes.sinaga10@mhs.if.its.ac.id

***Abstract*—Many companies in the world have used the business process management system (BPMS). This system is used to manage and analyze the running business process in the company. Every business process has a possibility to have changes in its realization. Those changes generate some variations of the business process. The variations, can be in line with the company's principles and or become an anomaly for the company. These anomalies can cause frauds which make some losses for the company. In order to reduce the losses, business process anomaly detection method is needed. This paper proposed ontology-based process modeling to model and capture the business process anomalies and the method of multi-level class association rule learning (ML-CARL) to detect fraud in business process. From the experiment which have been done in this paper, the accuracy of 0.99 was obtained from the ML-CARL method. It could be concluded that ontology-based process modeling and the ML-CARL method can detect business process anomalies well.**

***Keywords—component; formatting; style; styling; insert (key words)***

## I. INTRODUCTION

Companies in the world have been using business process management system to organize and analyze the way of the company's business process work [1]. Business process of a company could change dynamically. Such change resulted variations in business process where some of it accordance with the standards and principles of the company and there are also some contain anomalies [2]. Anomalies of business process that lead to losses for the company may be regarded as fraud because the anomalies was committed intentionally for personal interests.

Fraud is a problem that threatens the world. There were 1,388 frauds caused losses of 1,4 billion US Dollars in 96 countries [3]. On average, companies lost seven percent of gross income each year. There were twenty percent of people in the company have never stolen, sixty percent of them rely on cases and opportunities, and the rest of twenty percent is really dishonest [4]. Fraud could happen because of anomalies to business process or operational procedure standards and data manipulation [5]. Fraud could be defined as crimes that use deception as a major modus operandi and include various aberrations by individuals or organizations [6]. If fraud not prevented and detected would cause large losses for companies. Therefore, research on techniques to detect fraud in business process is needed.

The detection of anomalies on business process could be done with analyzing two aspects, data and process. Data mining techniques such as Decision Tree, Neural and Bayesian Network and Support Vector Machine have been used in previous studies to analyze data contain within the process [7], [8], and [9]. The data was used as input and resulting pattern or model that could be used for detecting anomalies. However, these methods have limitations in detecting anomalies because these methods were not able to analyze the behavior of process control flow.

Other research in the detection of anomalies were done by process mining techniques. Process mining techniques is used to detecting anomalies by analyzing the running processes. Conformance checking is one of the techniques in the mining process that can be used to compare the actual process data with standard process model [10]. Another benefit of this technique is analysis of control flow [11]. The analysis of control flow is able to detect activity that passed, activity that inputted, and wrong order activity. Any aberrations could be viewed as a anomalies of process.

In this paper will be proposed detecting fraud in process of business case studies on bank credit application using Multi-Level Class Association Rule Learning with ontology-based process modeling. In the training phase, process mining techniques are used to capture the anomalies which appears in event logs generated by activity in the business process. Standard business processes defined as the Standard Operating Procedure (SOP) and event logs modeled in advance into ontology form. Then, conformance checking is done by comparing the ontology graph of standard business process with ontology graph of event logs. The comparison is done using the Semantic Web Rule Language (SWRL). Then, from the comparison process resulted anomalies data are then analyzed using a multi-level class association rule (ML-CARL) learning. Furthermore, the calculation of the rates of anomalies

is explained in this paper using the theory of fuzzy sets of multi-attribute decision making.

The remainder of this paper is structured as follows. Section 1 explains the essential need of this research – followed by Section 2 providing the summary of several related research. Section 3, furthermore, provides an exclusive explanation of the case study. Section 4 presents the proposed method, each step of which is elaborated further. Section 5 presents an evaluation procedure through an explanation about experimental design and result. At last, the conclusion of this paper in presented in Section 6.

## II. Related Literature

### A. Process-based Fraud

Process-based Fraud (PBF) refers to a fraud occurred in business process [12]. Based on the research concerning with PBF, attribute and patterns have been identified in order to describe PBF [13]. The results of PBF identification found the anomaly attributes/ fraudulent behaviors in business process that could be defined into the following 6 types based on the way of how the fraud has done.

1. Skipped Activity

As its name implies, it is a type of anomaly in which an activity in the standard business process as stated in SOP is supposed to be done but in fact, it is skipped [14]. The skipped activity can be divided into 2 parts based on the type of the skipped activity, i.e. Skipped Sequence for any activities including normal sequence and Skipped Decision for any activities as decision in which there are a decision making or event branching [13]

2. Wrong Throughput Time

It is a type of anomaly in which an activity is performed faster or longer than the time limit stated in SOP. It is divided into 2 parts – Wrong Throughput Time Min and Wrong Throughput Time Max.

3. Wrong Resource

It is a type of anomaly in which an activity is not done by someone that has a role in accordance with SOP.

4. Wrong Duty

It is a type of anomaly in which an official performs 2 or more different activities in one running process. This type is divided into 3 parts: Wrong Duty Sequence (occurred in sequence activity), Wrong Duty Decision (occurred in decision activity) and Wrong Duty Combine (occurred in sequence and decision activity).

5. Wrong Pattern

Wrong Pattern is a type of anomaly in which wrong sequence activity is unfit with the sequence of activity as stated in the standard business process.

6. Wrong Decision.

It is the type of anomaly in which a wrong decision making occurs and is unfit with the standard stated in SOP.

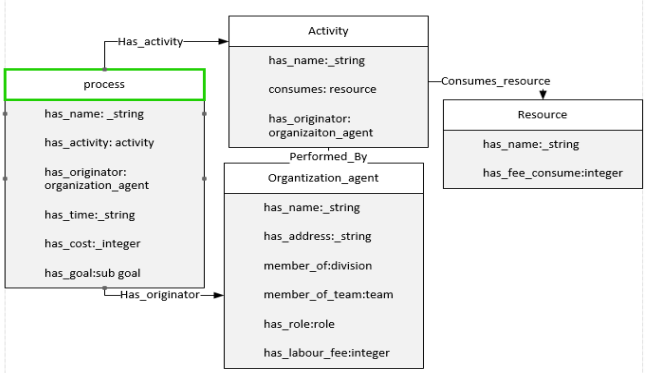


*Figure 1. Ontology-based event logs*

### B. Process Mining for Anomalies Detection

Process mining is a method which used to mine the process sequence in the event logs. According to [15], the objective of process mining was to extract some knowledge from event logs which recorded by the system. Process mining had three main activities were process discovery, conformance check and enhancement. In order to detect all of the anomaly attributes, process mining can assist by doing 4 analyzes: control flow analysis, role resource analysis, throughput time analysis and decision point analysis [14].

### C. Process Mining for Anomalies Detection

Kim et al [16] have introduced the enrichment of event logs by modeling them into ontology form. The goal was to add some external sources to event log so the hidden knowledge can be displayed in the event logs. This research have proposed the TOVE (Toronto Virtual Enterprise) framework. TOVE is the ontology integration which is used to support the enterprise modeling consisting of some concepts such as activity, organization, agents, cost, resource, etc.

**Table 1.**
**Form of SWRL atoms**

| Atom | Description |
|---|---|
| C(x) | C is declarations of class (class name) and x is name of individual or variable. |
| D(x) | D is declarations of data range and x is kind of variable or data value |
| P(x, y) | P is data or object property, x and y is kind of variable or OWL individual. If P is object property then y is kind of individual. And if P is data property then y is kind of data value |
| sameAs(x, y) | x and y is variable or individual, if and only if both of them are same individual |
| differentFrom(x, y) | x and y is variable or individual, if andonly if both of them are different individual |
| Builtln(r, $x_1,...x_n$) | R is built-in relation and $x_1,...x_n$ is kind of data value or variable. SWRL defines built-ins such as different kind of value comparisons. The correct sample are: equal(?x, y?), lessThan(?x, ?y) |

Example of the ontology-based event logs model can be seen in Figure 1. In Figure 1, there are four concept were resource, activity, organization-agent and process. Process is an additional concept that is added to TOVE to use information about process instance in event logs.

This paper will be use this ontology-based event logs model in order to modeling the standard business process model (SOP) and event logs into ontology form.

### D. *Process Mining for Anomalies Detection*

SWRL [17] is kind of OWL language that enhances with unary and binary statements. This rule consist of antecedent and consequent. Both of them consists of a set of atoms. If the antecedent is true then also consequent is true. The forms of atoms are define in this Table 1:

This is the example of SWRL rule [17] infers that x3 is the uncle of x1, if x2 is a parent of x1 and x3 is the brother of x2.

hasParent(?x1,?x2),hasBrother(?x2,?x3) -> hasUncle(?x1,?x3)

Signs "->" is use for conjunction between of antecedent and consequent atoms. "," is use for conjunction between atoms. Kind of variables are expressed by "?".

## III. CASE STUDY

In this paper, we would like to provide the example of the emergence of fraud in business process of credit application in bank. Figure 3 presents a business process of credit application in a bank. There are 25 activities consist of 17 sequence activities and 8 decision activities. The sequence activities were receive application, collateral verification locate, collateral local government, collateral government, collateral office, plafond estimation, decision director, decision leader, document verification adm, plafond verification adm, director otorization, leader otorization, loan reject, loan drowdone and gice info. And the decision activities were check completeness, check SID, check loan type, complete verification, check overrate, loan decision, make validation and plafond estimation. Duration time, resource and role have defined in each activity.

## IV. PROPOSED METHOD

The training section in this proposed method is implemented in two steps. First step is conformance checking by running the SWRL rules corresponded to each kind of anomaly attributes. Conformance checking is applied to detect anomalies in process. In that process, there are 6 kind of analyzes is done to detect the anomalies among process business. Second step is multi-level association rule learning applied to generate some anomaly association rules. These rules will be used for the testing section.

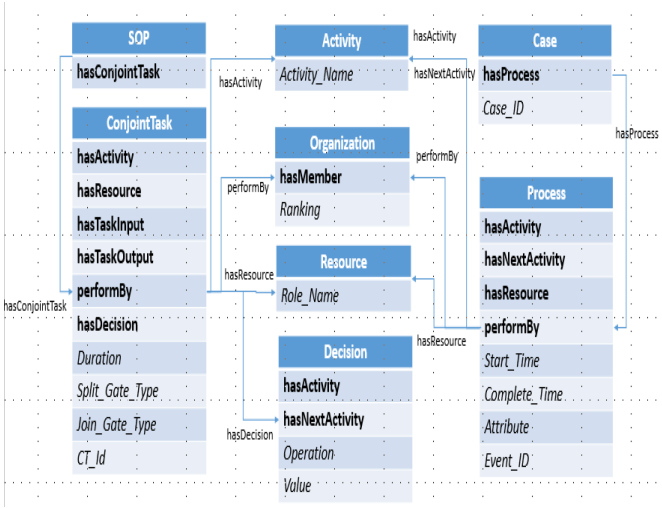


*Figure 2. Ontology model of standard business process*

### A. *Modelling Process Model and Event Log into Ontology-based*

According to TOVE framework which proposed by [16], standard business process model in the form of petri net (pnml) and the process instances which recorded in event logs (xes) will be modeled into ontology form. In this paper, the ontology model consists of eight concept were SOP, Conjoint Task, Activity, Organization, Resource, Decision, Case, and Process. SOP is a concept which represent the standard business process model which consist of some conjoint tasks. Conjoint Task is a concept for represent any activities which defined in the standard business process model. Activity is a concept to explain activities which are used in the conjoint task concept and the process concept. Organization is a concept which explain about the roles were defined in the business process. Resource is a concept which represent any resources which done any activities and process. Decision is a concept that explain any kind of decision making in standard business process model. Case is a concept that represent some instance processes. And process is a concept which represent every event which is done in a case. This model can be seen in Figure 2.

### B. *Conformance Checking using Anomalies Detection using SWRL Rule*

SWRL rule is an engine which can infers a new of knowledge from existing data in the model. SWRL rule can connect any part of model like classes, individual, object property, data property and etc become of integrated logic

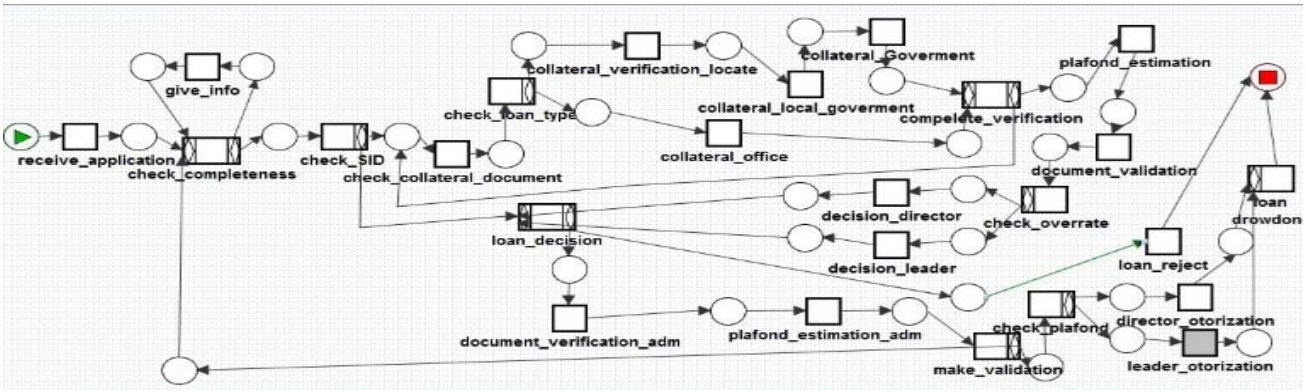


*Figure 3. Credit application business process model*

**Table 2**
**The importance levels of anomaly attributes**

| Levels | Fuzzy parameters | | | | Scales |
|---|---|---|---|---|---|
| | a | b | c | d | |
| Very Important (VI) | 0.7 | 1 | 1 | 1 | 100% - 70% |
| Important (I) | 0.5 | 0.7 | 0.7 | 1 | 100% - 50% |
| Fair (F) | 0.2 | 0.5 | 0.5 | 0.8 | 80% - 20% |
| Weak (W) | 0 | 0.3 | 0.3 | 0.5 | 0% - 50% |
| Very Weak (VW) | 0 | 0 | 0 | 0.3 | 0% - 30% |

relation. Anomaly that consist in event logs of data model are detected by compare two of main class, Case and SOP. Individual member of class Case has member of many events. Each of event is then compared with individual SOP that owned by class SOP. When any anomalies are founded, then new knowledge (inferrence data) will be pointed to member of class Anomali. Class Anomali member are kind of fraud attribut like *SkipSequence, SkipDecision, WrongThroughputTimeMin, WrongThroughputTimeMax,WrongResource, WrongDutySequence, WrongDutyDecision, WrongDutyCombine, Wrong Pattern dan Wrong Decision*. Inferrence data will be pointed ini these individuals.

SWRL rule is kind of static statement. Reasoner is kind of engine that can execute SWRL rule in order to operate this logic. This kind of process is called reasoning. In comprehensive definition reasoning is process of deriving valid deductions from an ontology model [18]. One of reasoner that mainly uses is Pellet. Pellet is freely available as Java API, is integrated in the latest version of Protege and supports SWRL rule [18].

In order to deriving and manipulating data inferrence there is kind of engine called OWL API. It is Java library for the web Ontology Language and RDF(S). The API provides classes and methodes to load and save OWL files, to query and manipulate OWL data models, and to perform reasoning based on Description Logic engines [19]. OWL API will get data inferrence that contains informations of kind anomalies. When the anomalies occured it will be signed in each case appropriate with kind of anomalies of it. If anomalies occured, it will be signed with flag 1. If no anomalies occured it will be signed with flag 0.

### *C. Fuzzy Set Multi Attribute Decision Making*

This method is used to determine the rates of anomaly from a set of anomalies occurred in a process. Two data are required in determining the rates of anomaly, i.e. the data of importance assessment to the attributes of PBF from the experts and the data of the occurrences of anomaly in the process originated from the result of conformance checking. Both two data are modeled into the number of fuzzy based on the table of importance and the level of its membership. For the data of importance assessment from the experts, the table of the importance level of anomaly attributes can be seen in Table 2 using the sample in [20].

**Table 3**
**The linguistic of occurrences**

| Attribute | a | b | c | d |
|---|---|---|---|---|
| Very Weak | 0 | 0 | 0.1 | 0.2 |
| Between Very Weak & Weak | 0 | 0.1 | 0.2 | 0.3 |
| Weak | 0.1 | 0.2 | 0.3 | 0.4 |
| Between Weak & Fair | 0.2 | 0.3 | 0.4 | 0.5 |
| Fair | 0.3 | 0.4 | 0.5 | 0.6 |
| Between Fair & Strong | 0.4 | 0.5 | 0.6 | 0.7 |
| Strong | 0.5 | 0.6 | 0.7 | 0.8 |
| Between Strong & Very Strong | 0.7 | 0.8 | 0.9 | 1 |
| Very Strong | 0.8 | 0.9 | 1 | 1 |

In this paper, the data of importance assessment from the experts has taken from the research conducted to the expertise audit of a bank. Based on the data, the weight measurement to each category/ attribute of anomalies is done. The weight value is divided into 4 parts: lower bound weight, middle weight 1, middle weight 2, and upper bound weight. The measurement of 4 weight values to each category could be done using Equation 1, Equation 2, Equation 3, and Equation 4.

$$\text{Lower Bound} = \frac{\sum_{k=1}^{n} a_k}{n} = \frac{0+0+0+0}{4} = 0 \quad (1)$$

$$\text{Middle Weight 1} = \frac{\sum_{k=1}^{n} b_k}{n} = \frac{0.3+0.3+0.3+0.3}{4} = 0.3 \quad (2)$$

$$\text{Middle Weight 2} = \frac{\sum_{k=1}^{n} c_k}{n} = \frac{0.3+0.3+0.3+0.3}{4} = 0.3 \quad (3)$$

$$\text{Upper Bound} = \frac{\sum_{k=1}^{n} d_k}{n} = \frac{0.5+0.5+0.5+0.5}{4} = 0.5 \quad (4)$$

Four equations above posse notation n as the number of experts and value a, b, c and d are the values of vector a, b, c and d in Table 2. In Table 2, the interval between 0-1 is divided accordingly by 5 category to determine the membership function parameters a, b, c, and d. Furthermore, for the data of process anomaly, table of level of the occurrences of anomaly attributes can be seen in Table 3. The interval between 0-1 is divided accordingly by 9 category to determine the membership function parameters a, b, c, and d. The next step is calculating the evaluation of the occurrences of anomaly attributes by using the same equation when calculating the importance weight. Further, from the result of the calculation of the importance weight of anomaly attributes and the degree of anomaly attributes, the calculation of final rating to calculate the weight of lower bound, middle1, middle 2, and upper bound was done by using Equation 5.

$$Final_{Rating} = \frac{1}{k} x[(S_{C1} x W_{C1}) + \cdots + (S_{Cn} x W_{Cn})] \quad (5)$$

where k refers to the number of categories, S refers to the degree of anomaly attributes, W refers to the weight of anomaly attributes in and Cn refers to anomaly attributes to n. As both four weights of final rating has been calculated, the rates of anomaly of a case is the summation of both four weights of the final rating. Further elaboration can be seen in Equation 6.

$$Rates\ of\ anomaly = Final\ Rating\ of Lower\ Bound + Final\ Rating\ of\ Middle1 + Final\ Rating\ of\ Middle2 + Final\ Rating\ of\ Upper\ Bound \quad (6)$$

The value of the rates of anomaly is then used for the process of searching the association rule using ML-CARL

### D. Fuzzy Set Multi Attribute Decision Making

Multi-level class association rule learning (ML-CARL) is a combined method between Multi-Level ARL (ML-ARL) and Class ARL (CARL). Multi-level ARL was the one of ARL enhancement method which used to seek association rules from multi-level data [21]. The goal is to generate complete rules. Whereas, CARL was the ARL enhancement method which aims to produce association rules in accordance with the requirements. The goal is the association rules that generated can be more efficiently. This CARL method classify the data into classes were defined first. Further, those classified data will be mine by ARL.

In this paper, an experiment to combine those both method in order to generates association rules completely and efficiently have done. Processed data is the anomalies data were captured in the process correspond to their rates of anomaly. The anomalies data is formed into a multi-level data as shown in Figure 4. Then, the anomalies data were classified into three classes, Non Fraud class, Semi Fraud class and Fraud class. This classification is done by using fuzzy membership that can be seen at Figure 5. The value parameter which used in this classification is the rates of anomaly of each case.

After the anomalies data were classified, the next step is mining association rule using ML-ARL. The steps of mining association rule are counting frequent item set and the support value, determine the value of minimum support, selecting item set which passed the minimum support, and calculate the value of confidence. In ML-ARL, these ARL' steps were done to each level of the data. So that the generated rules were the association rule of the first level and second level of the data. In ML-ARL method, there are two ways to determine the value of the minimum support, first, uniform support which is the value of the minimum support is same for all level. Second, reduced support which is the value of the minimum support is reduced at lower levels. In this research, uniform support is used to determine the value of the minimum support. The value of the minimum support in this research was set into 10 for all levels. The support's value could be calculated using Equation 7 and the confidence's value could be calculated using Equation 8.

$$\text{Support}(X, Y) = \left(\frac{\text{Transaction number contains } X \text{ and } Y}{\text{Transaction number}}\right) \quad (7)$$

$$\text{Confidence}(X, Y) = \left(\frac{\text{Transaction number contains } X \text{ and } Y}{\text{Transaction number contains } X}\right) \quad (8)$$

The association rules that generated by this method are association rules of anomalies which have consequent item of Non Fraud, Semi Fraud, or Fraud. This research did two ways of filtering rules in order to generate the appropriate rules [21]. These two ways of filtering rule were:

1. Removal of redundant rules.

To remove redundant rules, when a rule $R$ passes the minimum confidence, it is checked against every strong rule $R'$, of which $R$ is a descendant. If the confidence of $R$, $\varphi(R)$, falls in the range of the expected confidence with the variation of $\alpha$, it is removed.

2. Removal of unnecessary rules.

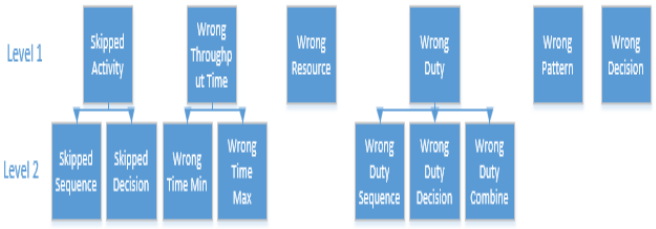


*Figure 4. Multi-level data of anomalies attribute*

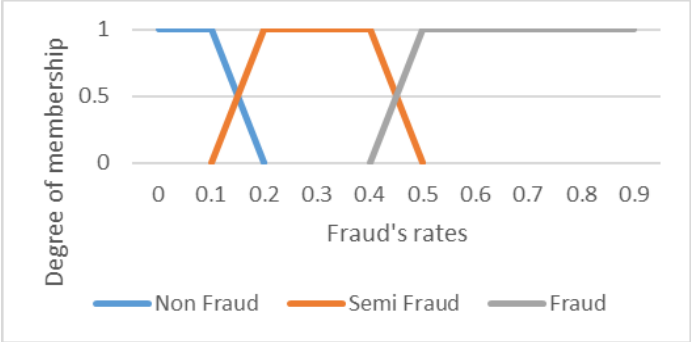


*Figure 5. Fuzzy membership for classification*

To filter out unnecessary association rules, for each strong rule $R'$: $A \Rightarrow B$, we test every such rule $R : A - C \Rightarrow B$, where C belongs to $A$. If the confidence of $R$, $\varphi(R)$, is not significantly different from that of $R'$, $\varphi(R')$, $R$ is removed.

## V. Evaluation

### A. Experimental Design

The evaluation in this research focuses on measuring the accuracy of the ML-CARL methods. The experiment has done to a case study of business process in bank credit application. The business process model can be seen in Figure 2. The dataset consists of training dataset and testing dataset which generated by some distribution models like in [14].

According to the analyze that have been done, anomaly against attributes can be modelled with the Poisson distribution with the parameter is set to 1. Poisson distribution is used because of its characteristic which in line with the business process fraud behavior. The number of cases of anomaly for each attribute is generated randomly based on the Poisson distribution. Therefore, each attribute has a different number of cases of anomaly of each month. Furthermore, there were 50 credit applications are processed each month. Then, anomalies is spread to each application based on the uniform (discrete) distribution. It aims to spread the anomalies in 50 credit applications on a month randomly and based on the number of anomaly occurrences for each attribute. Overall, there were 1200 cases produced as experimental data. Then, the experimental data is divided into training data and testing data. In training data, there are 1000 cases consist of 20 fraud cases, 14 semi fraud cases, and 966 legal/non fraud cases. In testing data, there are 200 cases

consist of 5 fraud cases, 3 semi fraud, and 192 legal/non fraud cases.

The conducted training generates association rules between the anomalous attributes. ML-CARL method produced 39 rules before filtering the rules while after filtering, can reduced the rules become only 24 rules. Further, the association rules with its confidence value is used in testing process to determine whether a case is fraud, semi fraud or legal/non fraud.

### *B. Experimental Result*

In order to measure the accuracy for both methods, measurement evaluation with Receiver Operating Characteristic (ROC) framework analyzes is done as in Equation 9. This accuracy measurement influenced by minimum confidence value of the association rule. There are 6 values that used in this measurement. First, True Positive (TP) value is the number of fraud cases which were detected as fraud by the method. Second, False Positive (FP) value is the number of semi fraud or non-fraud cases which were detected as fraud by the method. Third, True Semi Positive (TSP) value is the number of semi fraud cases which were detected as semi fraud by the method. Fourth, False Semi Fraud (FSP) value is the number of fraud or non-fraud cases which were detected as semi fraud by the method. Fifth, True Negative (TN) value is the number of non-fraud cases which were detected as non-fraud by the method. Sixth, False Negative (FN) value is the number of fraud or semi fraud cases which were detected as non-fraud by the method.

$$\text{Accuracy} \frac{TP+TSP+TN}{TP+FP+TSP+FSP+TN+FN} \qquad (9)$$

From the result of accuracy measurement, were obtained TP=5, TSP=2 and TN = 191, so ML-CARL method can obtain an accuracy at 0.99. Hence, can be seen that the ML-CARL method can detect fraud well with high accuracy.

## VI. CONCLUSION

According to the experiment result, it can be concluded that using ontology model to represent the standard business process model and event logs can be used to detect anomalies in the business process. It is supported by the SWRL Rule which used to checking the conformance between the standard business process model (SOP) and event logs. Therefore, ten types of anomaly attributes could be detected well by this method. Furthermore, multi attribute decision making (MADM) is reliable to calculate rates of anomaly according to the expert assessment and the occurrences of anomalies attribute. Hence, the ML-ARL method can generates association rules efficiently. This is supported by the accuracy value of 0.99 from the experimental results. Thus can be concluded that ML-CARL method can detects fraud well.

## REFERENCES


[1] J. Stoop, "A case study on the theoretical and practical value of using process mining for the detection of fraudulent behavior in the procurement process," in Process Mining and Fraud Detection, Netherlands, Twente University, 2012, pp. 22-63.

[2] R. Sarno, A.B. Sanjoyo, I. Mukhlash and H.M. Astuti, "Petri Net Model of ERP Business Process Variations for Small and Medium Enterprises," Journal of Theoretical and Applied Information Technology, vol. 54 No.1, August 2013, pp. 31-38.

[3] "Report to the Nations on Occupational Fraud and Abuse," ACFE, 2014, p.19.

[4] P. Goldman and H. Kaufman, Anti-Fraud Risk and Control Workbook, 2009, pp.11-22.

[5] M. Jans, N. Lybaert, K. Vanhoof, and J. M. van der Werf, "A business process mining application for internal transaction fraud mitigation," Expert Systems with Applications, vol. 38, 2011, pp. 13351-13359.

[6] Wells, J.T. Occupational Fraud and Abuse. Dexter, MI: Obsidian., 1997, p.221.

[7] F. Ogwueleka, Data Mining Application in Credit Card Fraud Detection System, Nigeria: Department of Computer Science, University of Abuja, 2011, pp.311-322.

[8] Ngai, E.W.T.,Yong Hu, Wong, Y.H., Chen Y.,Sun, X, "The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature," Decision Support Systems, vol. 50, 2011, pp. 559-569.

[9] Bhattacharyya, S., Sanjeev J., Tharakunnel, K., Westland, J.C, "Data mining for credit card fraud: A comparative study," Decision Support Systems, vol. 50, 2011, pp. 602-613.

[10] W.v.d.Aalst and A.K.A. Medeiros, "Process Mining and Security: Detecting Anomalous Process Executions and Checking Process Conformance," Computer Science, vol. 121, 2005, pp. 3-21.

[11] Gupta, S, W.M.P van der Aalst, A.J.M.M.Weijters, and A.K.Alves de Medeiros, Workflow and Process Mining in Healthcare, Eindhoven, 2007, p.159.

[12] M. Jans, N. Lybaert, K. Vanhoof, and J. M. van der Werf, "A business process mining application for internal transaction fraud mitigation," Expert Systems with Applications, vol. 38, 2011, pp. 13351-13359.

[13] S. Huda, R. Sarno, T. Ahmad, and H. A. Santoso, "Identification of Process-based Fraud Patterns in Credit Application", 2013, pp. 84-89.

[14] R. Sarno, R. D. Dewandono, T. Ahmad, M. F. Naufal and F. Sinaga, HybridAssociation Rule Learning and Process Mining for Fraud Detection, IAENG International Journal of Computer Science, 2015, pp. 59-72.

[15] W. v. d. Aalst, "Process Mining: Discovery, Conformance and Enhancement of Business Processes.," Springer, 2011, pp. 74-77.

[16] Thanh Tran Thi Kim, Hannes Werthner, "An Ontology-based Framework for Enriching Event-log Data," in *The Fifth International Conference on Advances in Semantic Processing*, Vienna, 2011, pp.110-115.

[17] Horrocks Ian et al. (2004, May) http://www.w3.org/. [Online]. http://www.w3.org/Submission/2004/SUBM-SWRL-20040521/

[18] Simon NIkles, "Expressiveness of Enterprise Modelling Languages", February 2010, pp. 29-30.

[19] Knublauch, Holger. Protégé wiki. [Online]. http://protegewiki.stanford.edu/wiki/ProtegeOWL_API_Programmers_Guide

[20] M. P. Barreiros, A. Grilo, V. Cruz-Machado, M. R. Cabrita, Applying Fuzzy Sets for ERP Systems Selection Within The Construction Industry, IEEE International Conference on Industrial Engineering and Engineering Management (IEEM), (2010), pp. 320 - 324

[21] Jiawei Han and Yongjian Fu, "Mining Multiple-Level Association Rules in Large Databases," in *IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING*, 1999, pp. 798-804.