Fraud Patterns Classification: A study of Fraud in business Process of Indonesian Online Sales Transaction

Solichul Huda
Department of Computer Science
University of Dian Nuswantoro
Semarang, Indonesia
solichul.huda@dsn.dinus.ac.id

Aripin
Department of Computer Science
University of Dian Nuswantoro
Semarang, Indonesia
aripin@dsn.dinus.ac.id

Mohammad Farid Naufal
Department of computer Science
Department of computer science
Surabaya, Indonesia
faridnaufal@staff.ubaya.ac.id

Vanny Martianova Yudianingtias
Department of Humanities
University of Dian Nuswantoro
Semarang, Indonesia
vannyningtias7@gmail.com

Anisti
Department Communications Science
University of Bina Sarana Informatika
Jakarta, Indonesia
anisti@bsi.ac.id

Abstract—Fraud detection has become an important research topic in recent years. In online sales transaction, fraud can occur on a business process. Fraud which occurs on business process is popularly known as process-based fraud (PBF). Previous studies have proposed PBF detection on process business model, however, false decisions are still often made because of new fraud pattern in online sales transactions. False decision mostly occurs since the method cannot identify the attributes of fraud in online sales transaction. This research proposes new fraud attributes and fraud patterns in online transactions. The attributes can be identified by exploring the event logs and Standard Operating Procedure (SOP) of online sales transactions. First, this is conducted by collecting event logs and creating SOP of online sales transaction; then, performing conformance between event logs and SOP; further, discussing with fraud experts about the result of SOP deviations which have been identified; moreover, determining convention value of the SOP deviation to fuzzy value, and classifying the SOP deviation; and at last, establishing fraud attributes and fraud patterns based on classification result. The new fraud attribute and fraud patterns are expected to increase accuracy of fraud detection in online sales transaction. Based on the evaluation, this method resulted a better accuracy 0.03 than the previous one.

Keywords— Fraud, pattern, classification, standard operating procedure, attribute, deviation

I. Introduction

Fraud is one of the loss causes experienced by both large and small companies. Fraud became a research theme trend nowadays because it causes a decrease in organizational and corporate revenue. It is predicted that fraud causes approximately 5% loss per year of their income [1]. The loss has reached more than 7 trillion US dollars. This loss has also been experienced by companies which use online transaction.

Companies and organization may experience a decrease in their profits since the anti-fraud system which they have cannot detect various fraud modes. The companies are possibly able to detect indications of fraud if the system can work optimally. For example, SOP violations done by employees, the company then can improve employee work system to minimize fraud incidents. In some cases, the solution can be in the form of testing the suitability of business processes with the SOP to analyze transaction data using a data mining approach, while to analyze a business process approach uses process mining.

Data mining to detect fraud has been carried out by several researchers in recent years, including by using neural network algorithm [2], a self-organizing maps algorithm [3], Dempster-Shafer theory [4] and Bayesian learning algorithms, classification models [5], empirical analysis and web service collaboration [6]. On the other hand, process mining to detect fraud has also been carried out by several researchers, by such methods as association role learning [7], hybrid ARL and process mining [8], Fuzzy MADM [9] and behavior models [10].

In 2018 fraud incidence in online transactions in Indonesia has reached more than one thousand five hundred cases. In online sales transactions, fraud detection method in [10] only obtained 85% accuracy. In contrast, in other objects, the method obtained 98% accuracy. This decreased accuracy may due to the fact that fraud attribute cannot investigate all SOP violations in online sales transactions. Thus, a fraud detection method is proposed in this paper based on SOP irregularities/deviations in online sales transactions. The identified SOP violations are defined as fraud attributes. In addition, this paper will investigate SOP violations in online sales transaction. Furthermore, the authors will also classify fraud patterns which occur and determine SOP violations weight. At last, the authors will determine whether SOP violation is categorized as fraud or not. The authors hypothesize that fraud pattern and the indicator or attribute of fraud proposed by this study are able to detect fraud in online sales transactions more accurately.

This paper is organized into seven sections. The first section elaborates the background of the study. The second section explains the research which has been previously done. Then, the third section describes identification of process mining and fraud detection. Fourth section explains case studies in this research. Section five describes the method proposes to detect fraud. Section six and section seven, contain the conclusions of the study and subsequent research which will be conducted.

II. Related Works

Fraud detection is considerably important to reduce the loss of company revenue caused by fraud. In online sales

transactions, this loss could be reduced by methods which may identify fraud before the payment process. This can be done by analyzing business process in online transactions. Process mining with several methods including performance, event sequence, control flow and role analysis possesses the ability to analyze business processes. In addition, fraud detection by process mining, merging data mining and process mining has been widely used in previous studies to detect fraud.

The research [11] has proposed process mining for fraud mitigation. The studies used performance analysis, control flow analysis, and role analysis to investigate business processes. These methods have proven that process mining can detect fraud in business processes. However, those researches have not used an algorithm to detect fraud.

The concept of 1 + 5 + 1 used a tool to detect fraud. This "1+5+1" consists of (1) log preparation + (5) {1} log analysis {2} process analysis, {3} conformance analysis, {4} performance analysis,{5} social analysis using filters, summarization, sorting , joining and aging + {1} iteration and refocusing. The study concluded that process mining can detect fraud in some business process models. However, this research has not yet resulted in fraud forms and fraud determination was subjectively conducted by the experts [12].

In a research [8], a combination of ARL algorithm and process mining method was proposed to detect fraud. In this study, ARL algorithm was used to identify the behavior of fraud perpetrators, while process mining was used to investigate SOP violations. This method generated rules and expert opinion for compliance checking with ARL. The study considered the weight of attributes, which were determined subjectively in deciding fraud.

Huda in [9] proposed a fuzzy approach to detect process mining based fraud. This method proposes a new attribute to detect fraud. This study conducted weighting violations and measured importance weighting on fraud attributes. Moreover, this study could investigate minor violations. However, fraud attributes offered in this study have not yet identified the originator's behavior.

A study conducted by [10] introduced behavioral models for fraud detection. The model was obtained by weighting the originator's behavior in running events and calculating the weight of the relation between the originators during the transaction. This method increased the accuracy of 0.02 to detect fraud in credit applications. However, this method only produced 0.85 accuracy to detect fraud in online transaction.

This research was conducted in Indonesia by using the event logs of some medium and small enterprises which serve online sales transactions. We obtained the logs from 3 (three) companies located in Surabaya, Yogyakarta and Jakarta. The event logs obtained were in the form of MXML format, thus it could be directly processed without doing any prior conversion.

Furthermore, the data of the event logs were normalized. This normalization was carried out to identify any redundant and incomplete data. Any identified data damage or double data were deleted to gain valid and reliable data. Then, the business process model of the online sales transactions were identified using ProM application. This business process model resulted from the ProM application was used as the basis of arranging the Standard Operating System (SOP). This study used WoPeD application for producing PNML file format to create the SOP. Moreover, the identification of fraud attributes in online sales transactions in this study was done by comparing the event logs and the SOP. A business process which violates the SOP was identified as suspicious Fraud.

III. PROCESS MINING AND FRAUD DETECTION

A. Process Mining

Process mining is a discipline focusing on extracting information from the event logs. Event logs are data about the processes carried out in a business process [13]. From these *event logs*, information about case ID, activity name, resource, start time stamp and complete time stamp will be obtained [14]. Besides, the event log data can be developed according to the necessary information.

Trace or business processes or instances are sets of execution sequences of events $\sigma \in E$ where each event is only one trace for $1 \leq i \leq j \leq |\sigma| : \sigma(i) \neq \sigma(j)$. In the trace, case code is usually defined, which is in the form of concepts and values. Furthermore, in a minimum event, concept, lifecycle, timestamp, activity and resource are defined. Resource or originator is the name of the executor who runs the event. Whereas the start and end times of running an event are indicated by the timestamp start and timestamps complete.

B. Standard Operating Procedure (SOP)

Online sales SOP consists of several data, i.e. flow, event name, and standard time of running the event The channel consists of several symbols, such as *xor split, xor joint* and *or*. The SOP can be written in various formats. Transition symbol indicates an event or operation (*xor* and etc), and place which describes the previous and subsequent transitions. In SOP arrangement, this research arranged SOP based on event logs using heuristic algorithms and ProM applications. Pro Mini application is able to create SOP in PNML format. Thus, this research can perform conformance event logs with SOP.

C. Process-Mining For Fraud Detection

There are three types of process mining: discovery, conformance, and enhancement (refinement) [15], [14]. Conformance method is used to investigate business process violations with SOPs [8], [9] . This research also uses conformance method by comparing business processes in the event logs with SOP. Then, the attribute values and importance weight of the attribute are determined based on the identified SOP violations.

Process-based Fraud (PBF) is fraud which occurs in a business process [9]. Detecting PBF in business process can be conducted in three different angles; from the perspective of business process, the role of the business, and from the perspective of the organization. This research detects fraud from the perspective of business processes. There are several advantages in using process mining to detect PBF. One of those is conformance checking that can be used to compare business processes with their SOPs. Another advantage of this method is the order in business processes

can be analyzed, and fraud in online sales transactions can be detected before the payment process is done.

D. Proposed Fraud Indicators / Attributes

Conformance method is used to analyze business process compared to SOP. Business process which violates SOP is identified as attribute or indicator of fraud. This study identified six types of SOP violations in the event logs of online sales transactions. This identification was obtained by analyzing event data training logs. The six types of deviations consisted of short throughput time, long throughput time, distance events, different patterns, wrong decisions and parallel events. Then by using formula 1, four of the six attributes were determined as fraud indicators or attributes. These four attributes were short throughput time, long throughput time, distance events, and different patterns. In addition, wrong decision attribute and parallel events are not categorized as fraud attributes since they did not have a significant stream of fraud events. The desciption of each SOP deviation is shown in Table 1.

$$r = \frac{n(\sum XY) - (\sum X)(\sum Y)}{\sqrt{[n(\sum X^2) - (\sum X)^2][n(\sum Y^2) - (\sum Y)^2]}} \qquad (1)$$

Where r is the value of the correlation coefficient, X is observation of variable X, Y is observation of variable Y, n is the pair's number of observations Y and X.

TABLE I. DESCRIPTION OF PBF ATTRIBUTES

Attribute	Description	Example
Throughput time short	The event execution time is shorter than low time tolerance	Event name / Standard time; Input order / 15 minutes. Execution of "input order" event takes only 8 minutes instead of 15 minutes
Throughput time long	The event execution time is longer than upper time tolerance	Execution of "input order" event takes 35minutes
Different pattern	A case pattern is different from that of the business process in SOP	D - E - F business process pattern; D - F - E Case pattern
Distant events	The distance between one event and the following event is longer than the standard time for executing the two events	Distance time execution of "See Item" and "Select Item" is more than time of standard events distance

E. Standard Event Time Determination

Throughput time analysis method is utilized to identify the time to execute an event which violates the SOP. Shorter or longer executing time than the standard time is considered to violate the SOP. In this study, standard time consists of standard time, lower tolerance time or upper tolerance time. In [9], the standard time to execute an event is determined as Eq. (2) below:

$$T_i = \overline{X_i} \pm (Tol_i + Ci_i) \qquad (2)$$

where Ti is the standard time to execute the event to I, Tol is tolerance time event to I, Ci is the confident interval value of event to i, and `X shows the average value to execute event to i. However, value¡⁻ (X_i) ^ in this study is replaced by the standard value event to i as specified in the SOP.

IV. CASE STUDY

Before this fraud is detected in online sales transaction. Online transaction business process is investigated to detect SOP deviations. Moreover, online transactions analysis is used to identify fraud attributes, importance weight of fraud attributes and fraud weights.

At first, the buyer will see a list of items offered. After that, the buyer chooses the method of purchase, i.e. transfer or cash on delivery (COD). Then, the buyer completes his/her identity consisting of name, address, city, contact number and email address.

When the buyer has decided to choose transfer payment model, the buyer then decides the type of payment, via mbanking or using an ATM. Moreover, the payment is conducted according to the payment model they prefer. The bank providing ATM or mbanking will send a report about the conducted payment process and information about the good shipping.

After the shipping process, receipt note or form of goods return will be sent. Receipt note provides information to the seller about the recipient's identity or return of goods. If a product is returned, the system will provide information about the type of goods and the reason for the return.

Event sequence, time to run, rule and transaction pattern are obtained by process mining after conducting business process analysis. If there is a sequence of business processes which is different from the SOP, then such different pattern attributes will be identified. If the time to run the event is too long or too short, the throughput time attribute can be identified. Indicators or attributes of fraud are identified as business processes which deviates from the SOP.

V. FRAUD DETECTION

A. Fraud Pattern Classification

The data in this study are event logs which served 10,000 online cases from 2016 - 2018. The event logs were in the form of digital data in MXML format which could be processed using web based applications. These event logs are divided into two parts, training data and testing data, in which there are 6,000 and 4,000 cases respectively. Training data were analyzed using such methods; throughput time analysis, different pattern analysis, and the distance events

analysis; of which distance events analysis method is proposed in this study.

Conformance which is performed on event logs and SOP is able to identify various indicators or attributes of fraud in some cases. In conducting conformance, this study applied throughput time analysis method, different pattern analysis, distant event analysis and skip analysis. After conducting conformance on event logs, there were 5 SOP violation identified, i.e. throughput time short (short throughput time), throughput time long (long throughput time), different pattern, distant event and skip. For instance, case code C00008 was identified as Throughput Time Long one dan different pattern one; case code C00229 was identified as Throughput Time Short two dan Throughput Time Long one, and so on. Table 2 shows the examples of identified SOP violation.

TABLE II.   EXAMPLE OF SOP VIOLATION

Case Code	Throughput Time Short	Throughput Time Long	Different Pattern	Distant Event	Skip
C00008		1	1		
C00042	2				
C00101				1	
C00229	2	1			
C00232		1			
C00285				1	
C00298	1			1	

Moreover, the number of each identified attribute violations is converted into attribute value in the form of fuzzy numbers with low, middle and high membership. Form of fuzzy numbers with low, middle and high membership. The function of fuzzy membership is the same as in study [9]. Case code C0008 has throughput time long low and different pattern low. Code C00229 has throughput time short middle and throughput time long low. The examples of SOP violation are presented in Table 3. In addition, the attribute values of each case are classified to illustrate the identified fraud patterns. Eq. 3 is used to classifying fraud patterns, as in [16].

TABLE III.   EXAMPLE OF SOP VIOLATION IN FUZZY

Case Code	Throughput Time Short	Throughput Time Long	Different Pattern	Distant Event	Skip
C00008		Low	Low		
C00042	Middle				
C00101				Low	
C00229	Middle	Low			
C00232		Low			

	Throughput Time Short	Throughput Time Long	Different Pattern	Distant Event	Skip
C00285				Low	
C00298	Low			Low	

$$d(x_i + x_j) = \sqrt{\sum_{r=1}^{n} (a_r(x_i) - (a_r(x_j))^2} \qquad (3)$$

Where $d(x_i + x_j)$ is eucledean distance, x_i is record i, x_j is record j, a_r is date r and i, j are 1,2,3… ets.

KNN algorithm is used to obtained shorten of distance value between data in training data. KNN algorithm is presented in Eq. 4, as in [17].

$$d_{mn}(x_1, x_2) = min_{1 \leq i \leq r, 1 \leq j \leq r} d(y_i, z_j)$$
(4)

This study was expected to classify the business process or any case violating the SOP. This classification would obtain the pattern of SOP violation from all existing business process in event logs. Code F001 is for throughput time short Low and different pattern Low. Code F002 means throughput time long Low and distant event Low. Finally, the expert assigns fraud weight to each fraud pattern. Fraud code F001 is given 10% weight, while F002 is given 20% weight. This fraud pattern weighing was conducted based on the experience of fraud experts. The examples of fraud patterns and fraud weights for each pattern are shown respectively in Table 4 and Table 5.

B. Fraud Detection in Online Sales Transaction Business Process

In a case or a process instance will end with a payment. Before carrying out the payment process, this detection method is done first. For example, there is an identified SOP violation in that case; accordingly, convert the violation into the attribute value. Based on fraud attribute, search for a table of fraud patterns, such as:

Find Throughput time short = low and event distance = middle

Then, fraud code "F007" pattern with 35% fraud weight will be obtained. To determine whether the case is fraud or not, compare fraud weight with threshold fraud value. This research found 0,45 threshold value. Thus, it can be determined that the case is not fraud or categorized as minor violation. However, if the fraud weight is above 0.45, this study confirms that the occuring SOP violations are included in fraud category.

TABLE IV.   FRAUD PATTERN IN ONLINE SALES TRANSACTION

Fraud Code	Throughput time Short	Throughput Time Long	Different Pattern	Distant Event	Skip
F001	Low		Low		
F002		Low		Low	
F003				Low	
F004	Middle				

F005		Middle			
F006				Low	High
F007	Low			Middle	

TABLE V.   FRAUD PATTERN AND FRAUD WEIGHTS

Fraud Code	Throughput time Short	Throughput Time Long	Different Pattern	Distant Events	Skip	Fraud
F001	Low		Low			10%
F002		Low		Low		20%
F003				Low		10%
F004	Middle					5%
F005		Middle				30%
F006				Low	High	90%
F007	Low			Middle		35%

	TP	FP	FN	TN	
Previous method	229	0	593	3178	0.85
The proposed method	352	0	470	3178	0.88

Evaluation on test data resulted in 822 cases of SOP violation. The results of the experts' discussion showed that the method in [8] resulted that 229 cases were identified as true positive, 593 cases as false positive, and 3178 cases as true negative. Meanwhile, by using this method, 352 cases were identified as true positive, 470 cases as false positive, and 3178 cases as true negative. The use of Eq. (5), the method in [8] resulted 0.85 accuracy, while the proposed method obtained 0.88 accuracy. The summary of the test data evaluation can be seen in the following Table 6.

VI. CONCLUSION

This study identified 5 fraud attributes in online sales transactions. Those fraud attributes are throughput time long, throughput time short, distant event, different patterns and skip. The findings of fraud attributes could increase the accuracy of fraud detection in online sales transactions. In addition, this study also identified 52 fraud patterns in online sales transactions. At initial investigation, the determination of SOP violation as fraud or not referred to the fraud patterns of which the weight was subjectively determined by the experts. Hence, the determination of fraud weight is significant for the accuracy in fraud detection. This study could identify new forms of SOP violation, i.e. distant event. This attribute has made the proposed method resulted better accuracy.

VII. SUGGESTION

This study is an initial research to detect fraud in online sales transactions. Future research shall conduct weighting attribute values, importance of attribute weight and determining fraud rating. The study is conducted in order to make fraud weighting can be automatically done by the system.

C. Experimental Result and Discussion

This research applied two methods of fraud analysis, the method proposed by in [8] and the method used in this study. These two methods were implemented to obtain the benefits of the proposed method. Moreover, evaluation process consists of two scenarios: (1) analyzing test data using internal methods [8], and (2) analyzing test data using methods proposed in this study. Then, the experts analyzed test data using their own methods. Accuracy evaluation of both methods was used to find out the benefits of the methods. In addition, Eq. (5) was used to calculate the accuracy of the methods.

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \qquad (5)$$

This research used fuzzy approach to investigate SOP violations as a fraud or not. Furthermore, this fuzzy approach was also used in the evaluation stage to analyze test data.

Receiver operating characteristics (ROC) was used to measure the accuracy of fraud detection method. Such accuracy measurement was conducted by concerning on true positive (TP), true negative (TN), false positive (FP), and false negative (FN). TP was used to state that the experts and the method resulted in a similar conclusion of a case as a fraud. Meanwhile, TN is used to refer to the fact that the experts and this method resulted in the same statement that a case in not a fraud. On the other hand, when the experts defined a case as a fraud and the method concluded not as a fraud, it belonged to FN. Besides, when the experts stated that a case was not a fraud, instead the method stated that the case was not a fraud, then it can be categorized as FP.

TABLE VI.   RESULT OF TEST DATA EVALUATION

Method	ROC variable	Accuracy

REFERENCES

[1] E. W. T. Ngai, Y. Hu, Y. H. Wong, Y. Chen, and X. Sun, "The Application of Data Mining Techniques in Financial Fraud Detection: A Classification framework and an Academic Review of Literature". Decision Support Systems, Vol. 50, No. 3, pp. 559-569, 2010.

[2] D. R. Kalyani and D. U. Devi, "Fraud Detection of Credit Payment System by Genetic Algorithm", International Journal of Scientific & Engineering Research, vol. 3, no. 7, (2012), pp. 1-6.

[3] V. Zaslavsky and A. Strizhak, "Credit Card Fraud Detection Using Self-Organizing Maps", Information & Security, vol. 18, (2006), pp. 48-63.

[4] S. Panigrahi, A. Kundu, S. Sural, and A.K. Majumdar, "Credit Card Fraud Detection: A Fusion Approach Using Dempster-Shafer Theory and Bayesian Learning", Information Fusion, vol. 10, no. 4, (2009), pp. 354-363.

[5] A. Shen, R. Tong and Y. Deng, "Application of Classification Models on Credit Card Fraud Detection", Proceedings of 2007 International Conference on Service System and Service Management, IEEE, Chengdu, China,(2007) June 9-11.

[6] A. Shen, R. Tong and Y. Deng, "Application of Classification Models on Credit Card Fraud Detection", Proceedings of 2007 International Conference on Service System and Service Management, IEEE, Chengdu, China,(2007) June 9-11.

[7] S. Huda, R. Sarno, T. Ahmad, H. A. Santosa, "Identification of Process-based Fraud Paterns in Credit Application", 2 nd

International Conference on Information and Communication Technology (ICoICT), (2014) June 28-29.

[8] R. Sarno, D. R. Dewandono, T. Ahmad, M. F. Naufal and F. Sinaga, "Hybrid Association Rule Learning and Process Mining for Fraud Detection", IAENG International Journal of Computer Science, vol. 42, no. 2, (2015), pp. 59-72.

[9] S. Huda, R. Sarno and T. Ahmad, "Fuzzy MADM approach for Rating of Process-based Fraud", Journal ICT. Research Application, vol. 9, no. 2, (2016), pp. 111-128.

[10] S. Huda, R. Sarno and T. Ahmad, "Increasing Accuracy of Process-based Fraud Detection Using A Behavior Model", International Journal of Software engineering and its application, vol. 9, no. 2, (2015), pp. 111-128.

[11] M. Jans, M. J. van der Werf, N. Lybaert and K. Vanhoof, "A Business Process Mining Application for Internal Transaction Fraud Mitigation", Expert Systems with Applications, vol. 38, no. 10, (2011), pp. 13351-13359.

[12] J. J. Stoop, "Process Mining and Fraud Detection", Thesis, Business Information Technology Department, Twente University, Enschede, Netherlands, 2012.

[13] R. Sarno, P. L. I. Sari, H. Ginardi, D. Sunaryono , I. Mukhlash, "Decision Mining For Multi Choice Workflow Patterns", International conference on Computer, Control, and Its Application, (2013) November 19-21.

[14] W. M. P. van der Aalst, "Discovery, Conformance and Enhancement of Business Processes", Springer, pp. 7-8, (2010).

[15] W. M. P. van der Aalst and A. K. A. de Medeiros, "Process Mining and Security: Detecting Anomalous Process Executions and Checking Process Conformance", Electronic Notes in Theoretical Computer Science, vol. 121, (2005), pp. 3-21.

[16] J. Han and M. Kamber, Data Mining : Concept and Techniques. New York, Morgan Kaufmann Publisher, 2006.

[17] G. Goujon, Chaoqun, and W. Jianhong, Data Clustering :Theory, Algorithms, and Applications. Virginia, ASA, 2007.

Browse ⌄   My Settings ⌄   Help ⌄   Institutional Sign In

Institutional Sign In

All   ⌄   🔍
☐   ADVANCED SEARCH

Quick Links
Search for Upcoming Conferences
Browse Conferences > Mechanical, Electronics, Compu... > 2020 3rd International Confere...   ❓
IEEE Publication Recommender
IEEE Author Center

Mechanical, Electronics, Computer, and Industrial Technology (MECnIT), International Conference on
Proceedings
The proceedings of this conference will be available for purchase through Curran Associates.

Mechanical, Electronics, Computer, and Industrial Technology (MECnIT), 2020 3rd International Conference on   🌐   ☰   ➕

Print on Demand **Purchase at Partner**
🌐 Copy Persistent Link   ☰ Browse Title List   ➕ Sign up for Conference Alerts

| **Proceedings** | All Proceedings | Popular |

2020 3rd International Conference on Mechanical, Electronics, Computer, and Industrial Technology (MECnIT) DOI:
doi   10.1109/MECnIT48290.2020

Search within results   Per Page: ⌗Per Page 25 | Export | Email Selected Results

Showing **1-25** of **85**
🔻 Filter   sort: ⌗Sort Sequence | ✉ Email

Refine

Author ⌄

Affiliation ⌄

Conference Location ⌄

Quick Links
Search for Upcoming Conferences
IEEE Publication Recommender
IEEE Author Center

Proceedings
The proceedings of this conference will be available for purchase through Curran Associates.

Mechanical, Electronics, Computer, and Industrial Technology (MECnIT), 2020 3rd International Conference on

☐ **Analysis of Critical Success Factors on ERP Implementation in PT. Toyota Astra Motor Using Extended Information System Success Model**
Safira Aini; Muharman Lubis; R. Wahjoe Witjaksono; Anik Hanifatul Azizah
Publication Year: 2020 , Page(s): 370 - 375
Cited by: Papers (1)

☐   Abstract   (637 Kb)
Analysis of Critical Success Factors on ERP Implementation in PT. Toyota Astra Motor Using Extended Information System Success Model
Safira Aini; Muharman Lubis; R. Wahjoe Witjaksono; Anik Hanifatul Azizah
2020 3rd International Conference on Mechanical, Electronics, Computer, and Industrial Technology (MECnIT)
Year: 2020

☐ **Search Query Clustering Comparation On E-Commerce Using K-Means And Adaptive DBSCAN**
Darwin; Ronsen Purba; Muhammad Fermi Pasha
Publication Year: 2020 , Page(s): 207 - 211

☐   Abstract   (945 Kb)
Search Query Clustering Comparation On E-Commerce Using K-Means And Adaptive DBSCAN
Darwin; Ronsen Purba; Muhammad Fermi Pasha

2020 3rd International Conference on Mechanical, Electronics,
Computer, and Industrial Technology (MECnIT)
Year: 2020

☐ **The Object Detection on Video Transmission over Wireless
Visual Sensor Network**
Kalvein Rantelobo; Hendro F. J. Lami; Andreas C.
Louk; Bernandus; Nyoman P. Sastra
Publication Year: 2020 , Page(s): 54 - 57

☐   Abstract   (1029 Kb)
The Object Detection on Video Transmission over
Wireless Visual Sensor Network

Kalvein Rantelobo; Hendro F. J. Lami; Andreas C.
Louk; Bernandus; Nyoman P. Sastra
2020 3rd International Conference on Mechanical, Electronics,
Computer, and Industrial Technology (MECnIT)
Year: 2020

☐ **EMG Based Control of a Quadcopter**
Maham Ali; Areeba Riaz; Waleef Ullah Usmani; Noman Naseer
Publication Year: 2020 , Page(s): 250 - 254

☐   Abstract   (756 Kb)
EMG Based Control of a Quadcopter

Maham Ali; Areeba Riaz; Waleef Ullah Usmani; Noman Naseer
2020 3rd International Conference on Mechanical, Electronics,
Computer, and Industrial Technology (MECnIT)
Year: 2020

☐ **Characterizing the Effect of Motion Class Taxonomy on the
Performance of Hand Motion Classifiers**
Waseem Shahzad; Yasar Ayaz; Muhammad Jawad Khan; Noman
Naseer; Amad Zafar
Publication Year: 2020 , Page(s): 58 - 63

☐   Abstract   (1765 Kb)
Characterizing the Effect of Motion Class Taxonomy
on the Performance of Hand Motion Classifiers

Waseem Shahzad; Yasar Ayaz; Muhammad Jawad Khan; Noman
Naseer; Amad Zafar
2020 3rd International Conference on Mechanical, Electronics,
Computer, and Industrial Technology (MECnIT)
Year: 2020

☐ **Control of Two-Link Robot Manipulator with Uncertainty
Parameter using Self-Tuning Sliding Mode Control**
Anisa Ulya Darajat; Swadexi Istiqphara
Publication Year: 2020 , Page(s): 376 - 380

☐   Abstract   (1016 Kb)
Control of Two-Link Robot Manipulator with
Uncertainty Parameter using Self-Tuning Sliding
Mode Control

Anisa Ulya Darajat; Swadexi Istiqphara
2020 3rd International Conference on Mechanical, Electronics,
Computer, and Industrial Technology (MECnIT)
Year: 2020

☐ **Fraud Patterns Classification: A study of Fraud in business
Process of Indonesian Online Sales Transaction**
Solichul Huda; Aripin; Mohammad Farid Naufal; Vanny Martianova
Yudianingtias; Anisti
Publication Year: 2020 , Page(s): 212 - 217

☐   Abstract   (988 Kb)
Fraud Patterns Classification: A study of Fraud in

1   2 3 4 >

IEEE Account

» Change Username/Password

» Update Address

Purchase Details

» Payment Options

» Order History

» View Purchased Documents

Profile Information

» Communications Preferences

» Profession and Education

» Technical Interests

Need Help?

» **US & Canada:** +1 800 678 4333

» **Worldwide:** +1 732 981 0060

» Contact & Support

All ▾

🔍
ADVANCED SEARCH

Conferences   >   2020 3rd International Confer...   ⓘ

Fraud Patterns Classification: A study of Fraud in business Process of Indonesian Online Sales Transaction

Publisher: IEEE | Cite This | PDF

Solichul Huda ;   Aripin ; Mohammad Farid Naufal ;   Vanny Martianova Yudianingtias ;   Anisti   **All Authors**

46
Full
Text Views

⊰ Export to
Collabratec   **Alerts**

Manage
Content Alerts

Add to Citation
Alerts

Abstract

Document Sections

I.   Introduction

II.   Related Works

III.   Process Mining
and Fraud
Detection

IV.   Case study

V.   Fraud Detection

Show Full Outline ▾

Authors

References

Keywords

Metrics

More Like This

Downl
PDF

Abstract: Fraud detection has become an important research topic in recent years. In online sales transaction, fraud can occur on a business process. Fraud which occurs on business... **View more**

▾ Metadata
Abstract:
Fraud detection has become an important research topic in recent years. In online sales transaction, fraud can occur on a business process. Fraud which occurs on business process is popularly known as process-based fraud (PBF). Previous studies have proposed PBF detection on process business model, however, false decisions are still often made because of new fraud pattern in online sales transactions. False decision mostly occurs since the method cannot identify the attributes of fraud in online sales transaction. This research proposes new fraud attributes and fraud patterns in online transactions. The attributes can be identified by exploring the event logs and Standard Operating Procedure (SOP) of online sales transactions. First, this is conducted by collecting event logs and creating SOP of online sales transaction; then, performing conformance between event logs and SOP; further, discussing with fraud experts about the result of SOP deviations which have been identified; moreover, determining convention value of the SOP deviation to fuzzy value, and classifying the SOP deviation; and at last, establishing fraud attributes and fraud patterns based on classification result. The new fraud attribute and fraud patterns are expected to increase accuracy of fraud detection in online sales transaction. Based on the evaluation, this method resulted a better accuracy 0.03 than the previous one.

Published in: 2020 3rd International Conference on Mechanical, Electronics, Computer, and Industrial Technology (MECnIT)

Date of Conference: 25-27 June 2020

INSPEC Accession Number: 19890153

Date Added to IEEE *Xplore*: 14 August 2020

DOI: 10.1109/MECnIT48290.2020.9166644

Publisher: IEEE

ISBN Information:

Conference Location: Medan, Indonesia

No metrics found for this document.

☰ Contents

I. Introduction

Fraud is one of the loss causes experienced by both large and small companies. Fraud became a research theme trend nowadays because it causes a decrease in organizational and corporate revenue. It is predicted that fraud causes approximately 5% loss per year of their income [1]. The loss has reached more than 7 trillion US dollars. This loss has also been experienced by companies which use online transaction.

Sign in to Continue Reading

Authors	⌄
References	⌄
Keywords	⌄
Metrics	⌃

Usage ❓

| 2021 | 2020 |
| | |

Jan	Feb	Mar	Apr	May	Jun	
2	-	4	-	-	-	**46**
Jul	Aug	Sep	Oct	Nov	Dec	Total usage since Aug 2020
-	-	-	-	-	-	

Best Month: Mar　　　　　Year Total: 6
* Data is updated on a monthly basis. Usage includes PDF downloads and HTML views.

Citations ❓

Search for
Citations in
Google Scholar®