Sequential Anomaly Detection Techniques in Business Processes

Christian Linn(✉) and Dirk Werth

AWS-Institute for Digitized Products and Processes, Saarbrücken, Germany
{christian.linn, dirk.werth}@aws-institut.de

Abstract. Many companies use information systems to manage their business processes and thereby collect large amounts of transactional data. The analysis of this data offers the possibility of automated detection of anomalies, i.e. flaws and faults, in the execution of the process. The anomalies can be related not only to the sequence of executed activities but also to other dimensions like the organization or the person performing the respective activity. This paper discusses two approaches of detecting the different anomalies types using basic sequential analysis techniques. Besides the classical one-dimensional approach, a simple approach to use multiple dimensions of the process information in the sequential analysis is discussed and evaluated on a simulated artificial business process.

Keywords: Anomaly detection · Business process · Business analytics

1 Introduction

Nowadays many companies use software systems, so called Process Aware Information Systems (PAIS), to manage their internal business processes [1]. As a consequence, transactional data from each individual execution of a process can be logged and documented. The process data is recorded in event logs which typically contain information about the executed activities such as the type of the activity, the time at which an activity was executed and the organization or person who performed the task [2]. The availability of such event logs offers the opportunity for data driven analyses of business processes. A related research field using this data resource is process mining which adopted data mining techniques to extract process-related information and discover, verify or improve a process model [3]. Of increasing interest is the use of process data for the detection of anomalies, i.e. flaws and faults that happen during the process execution [4]. Especially in cases where the process is not strictly predefined by an existing model but allows some flexibility or exceptions in execution, anomaly detection can be helpful to identify or avoid situations which are potentially harmful for a company [5]. These anomalies can be of various types and appear in different parts of the process, e.g. in the sequence of the executed activities or in the organization unit that performs a certain task. Most of the existing anomaly detection techniques for business processes concentrates on the detection of anomalies in the sequence of the executed activities (e.g. in [6, 7]).

W. Abramowicz et al. (Eds.): BIS 2016 Workshops, LNBIP 263, pp. 196–208, 2017.
DOI: 10.1007/978-3-319-52464-1_18

The following paper investigates basic sequential analysis techniques to detect anomalies in other dimensions of the process data. In addition a simple approach to use multiple dimensions of process information is presented and discussed. To demonstrate the concepts, an artificial process data set is simulated containing anomalies in the activity sequence as well as in the assignment of the acting persons that perform the activities. The performance of three sequential analysis techniques are compared to gain insights in the pros and cons of using the one- and multidimensional approaches.

The structure of the paper is as follows: First some special characteristics of anomalies in business processes are discussed followed by a summary of existing research relevant to this topic. Then the strategy of the presented research is outlined. The simulation of the artificial business process data set and the details of the detection techniques are presented in the next chapters. Then the results of the comparison between the different analysis approaches are discussed followed by an interpretation and a final conclusion.

2 Anomalies in Business Processes

Anomalies can be seen in the most general way as deviations from a defined normal behavior [8]. For business processes, the main characteristics of the anomaly detection problem is the sequential nature of the data. The transactional data that is saved in the event logs usually contains information about many executions of the same process. Throughout this paper a process execution is referred to as instance of a business process. Each process instance again consists of a set of activities, i.e. events or tasks that were performed during the execution. Each activity is usually related to a moment in time at which the activity was executed. Therefore each instance of a business process can be seen as a sequence of activities [9]. Typically, each activity can in addition be related to several dimensions of data, for example information about the person who performed the activity, the organization unit or the financial budget for an activity. Therefore, several types of anomalies are possible in business processes (e.g. in [5]):

- Anomalies can occur in the sequence of activities in a process instance. Thereby, either the full process instance or subparts of the sequence can be anomalous with respect to the rest of the data. In this context, anomalous instances are often executions that happen infrequent compared to the rest of the process executions.
- Anomalies could also be present in the time dimension of a process. Either the duration of a single activity or the time behavior of the activity sequence may be anomalous.
- Anomalies can occur in the organizations or persons that perform the activities. This can for example include cases where an activity is executed by the wrong person or where the sequence of involved organizations does not correspond to the normal case. Similar to the organization and persons, other data dimension of a business process could be anomalous, for example the financial budget related to an activity.

- In many cases, a business process is accompanied with some sort of data transfer, e.g. documents, products or any other information. Anomalies can also be irregularities in this data transfer.
- Finally, there can also be cases of multidimensional anomalies, where irregularities only occur in the combination of different dimensions. An example would be when a sequence is in principle allowed but must be accounted as anomaly in case it is executed by a certain person at a certain time.

3 Previous Work

Anomaly detection is a topic with high attention and research interest in various domains. Especially in areas like financial fraud detection [10], fraud detection in healthcare [11] and network intrusion detection [12], automated anomaly detection plays an important role.

For anomaly detection in business processes, most of the literature concentrates on the development of new detection techniques for sequential anomalies. The existing detection techniques can be divided into two categories: Methods using process mining techniques to discover an underlying process model and check its conformance with the data and methods that do not require a description of a process model but instead use generic data mining techniques to investigate the anomalies.

A general concept of using process mining for anomaly detection was discussed in [2] where only normal process instances were used to discover a process model. Anomalies are detected by determining the conformance between this model and new test instances. In [6, 13, 14] the authors overcome the need for a training set with only normal instances and propose three algorithms that can dynamically detect anomalies, based on the assumption that anomalies happen only rarely compared to normal instances. Sarno et al. use an ontology-based process model discovered from a training sample and define multi-level association rules based on this to identify anomalies in the test sample [15].

In the second major approach for detecting business process anomalies, data mining techniques are used to detect anomalies without constructing a descriptive model. In [16] the authors train a local outlier factor (LOF) algorithm to predict anomalies in future process instances. Cabanillas et al. use a Support Vector Machine trained on classified input data for real-time monitoring of processes [17]. In [7] the authors propose an approach to use Variable Order Markov Models to detect sequential anomalies. A sequence is defined as anomalous if at least one activity of the sequence is predicted with a probability value lower than a certain threshold. Finally, the authors of [18] compare a windows based and a Markovian based detection technique to identify anomalous sequences.

Only few approaches exist which also address anomalies that are not solely related to the activity sequence. In [19] the authors propose a genetic based algorithm to discover a process model and combine this with a set of rules to characterize attacks on an organization performing the activities in a process. The authors of [20] discuss an approach to detect temporal anomalies by first constructing a process model that

contains statistical information about the execution times of activities and second using a hypothesis test to identify anomalies in the activity durations. Quan et al. propose to transform process data in a multidimensional feature space and construct a hyper-sphere, similar to the concept of support vector classifiers [21]. The hyper-sphere is determined from a training set where they assume that normal behaving data is much more frequent than outliers. Each test data instance lying outside this hyper-sphere is then classified as anomaly. Accorsi et al. [22] present an approach for a forensic analysis of business process logs against data flow policies. It uses propagation graphs (directly labeled graphs extracted from event log) to capture data flow in process executions and verifies with external data flow rules whether a process executions is acceptable or not.

4 Research Strategy

The existing research on anomaly detection in business processes mainly concentrates on the development of new detection techniques for anomalies in the activity sequence. One possible way for this is to use sequential data mining techniques, as for example discussed in [23], to determine the anomalous sequences or subsequences. Anomalies in other data dimension like the execution time or the responsible organization are only rarely addressed. The aim of this paper is to discuss and compare different approaches of sequential anomaly detection to identify anomalies not only in the activity sequence but also in other dimensions of business process data. Two different approaches are investigated:

- A classical one-dimensional method where the sequence of a single process data dimension is used. The standard approach is to consider the activity sequence in order to identify anomalies in the process execution. But also with other data dimension, such as the involved organization unit or the responsible person, this approach can be useful and might even be sensitive to more types of anomalies. Anomalies in the one-dimensional sequence of the responsible persons could for example be related to either a wrong person executing an activity in a normal activity sequence, or to a wrong sequence of activities resulting in a wrong sequence of acting persons.
- A multidimensional approach that combines information from two or more data dimension of a process execution and is then used in a sequential analysis. An example would be to combine the activity information with the information of the related acting person. In this case, an activity performed by "*Person A*" would be treated as a different element in the sequential analysis than the same activity performed by "*Person B*".

In order to demonstrate the different concepts and to obtain quantitative and comparable results for the different approaches, three basic sequential anomaly detection techniques are used and applied to a simulated artificial business process data. The simulated data represents a typical sales process and contains information about the process activities as well as the involved persons. Anomalies are included in the

activity sequence, in the way persons are assigned to activities and in the combination of both.

5 Simulation of Business Process Data

In order to get a reliable understanding on how the anomaly detection techniques perform for business process data with the different type of anomalies, an artificial data set is simulated. This allows a quantitative evaluation of the methods, as the normal and anomalous instances are generated in a controlled way. Special techniques for simulating business process data, have for example been used in [7, 19]. These techniques allow the generation of random business process data based on user-defined input parameters [24]. Details on the characteristics of the simulated process and the incorporation of anomalies were however not discussed but can have a significant impact on the performance of the chosen detection technique.

For this paper a slightly different simulation approach was implemented to provide a maximum transparency in the way anomalies are generated. It is a simple probabilistic approach that allows a detailed definition of transitions between process activities and the type and frequency of the generated anomalies. As an example, a typical sales process in a company was simulated, including a low frequency of anomalous instances. Figure 1 shows a sketch of the simulated process. It consists of 13 different activities (boxes). The arrows in the diagram show the transitions between the activities that are allowed in a normal process execution, together with the chosen transition probabilities. Each instance starts with activity *"Create Order"*. The next activity in the instance is randomly chosen, respecting the allowed transition probabilities. This is repeated until the instance reaches the activity *"Close Order"*. For example, if the instance after the second step consists of the sequence *"Create Order"* - *"Check customer account"* then the next activity is at 20% probability *"Create new account"* and at 80% probability *"Send order confirmation"*. For each activity a set of responsible persons is defined who can execute the respective activity. A sketch of the relation between persons and activities is given in Fig. 2. The assignment of a specific person to an activity is done randomly for each process instance, following the defined probabilities given in Fig. 2. For example the activity *"Send Order Confirmation"* is in 80% of the cases performed by person *"Sales/B"* and in 20% of the cases by person *"Sales/C"*. Finally, when the state *"Close order"* is reached the instance is completed and the simulation of the individual process execution terminates.

In addition to the normal and allowed process instances, a low probability of anomalous executions is included. Three types of anomalies are simulated: anomalous transitions in the activity sequence, anomalies in the assignment of persons to a specific activity and combinations of both cases. Each step in the simulation of a process instance is with a probability of $p_{fail} = 0.1\%$ declared as anomaly. If a step is labeled as anomalous, in 50% of the cases an anomaly in the activity sequence is generated. The respective activity is randomly chosen from all but the allowed activities. As an example this would mean that after the sequence *"Create Order"* - *"Check customer account"* any activity could follow, except *"Create new account"* and *"Send order confirmation"*. A possible next activity could be *"Order goods"*. In 40% of the

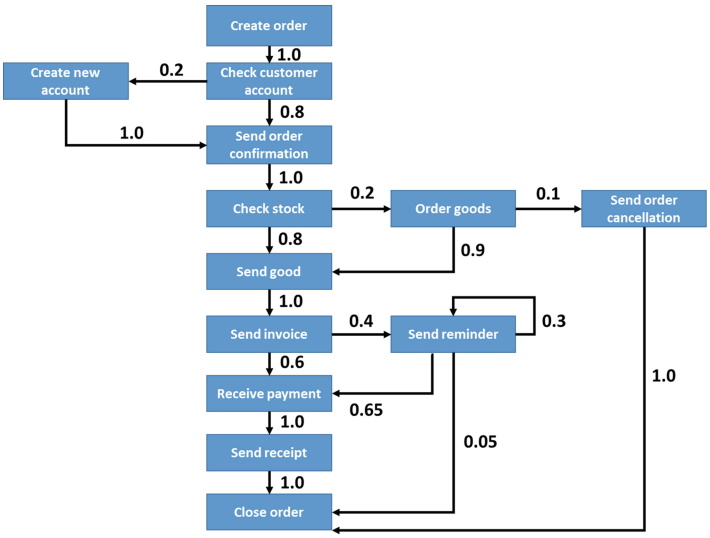

Fig. 1. Model of the simulated business process

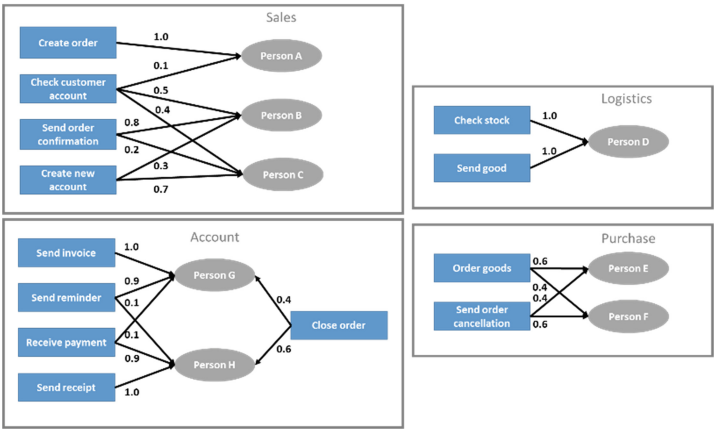

Fig. 2. Assignment of responsible persons to the process activities

anomalous process steps, an anomaly in the acting person is simulated by randomly choosing a person from all but the allowed persons for this activity. An example would be to assign person *"Sales/C"* to activity *"Check stock"*. Finally, in 10% of the anomalous process steps, both the activity as well as the acting person are chosen in the described non-normal way.

As the anomaly probability p_{fail} is included in each step of the sequence, it can happen that more than one anomalies appear in a single process execution. A completed process instance is labeled as an anomaly if at least one anomalous transition occurred during the simulation.

Following this recipe, 30000 independent instances of this process are simulated. In total 259 anomalous instances are present in the full data sample, 132 in the activity sequence, 88 in the assigned person and 39 anomalies in both, activity and related person. It should be noted that this simulation technique, does not give strict restrictions to the type of anomalies. In fact, due to the random character of the anomalous transitions, a wide spectrum of non-normal process instances is possible.

6 Sequential Analysis Techniques

For this research, three different sequential techniques are used to detect anomalies in business processes: a windows based, a Markov based and a Hidden Markov based method. The motivation to use these methods is that they can operate in an unsupervised way, i.e. without a training sample containing knowledge about the nature (normal or anomaly) of the single sequences. In addition they are more sensitive to anomalies in short subsequences of the process instances compared to other sequential techniques, like Nearest Neighbor Methods [23]. With the discussed simulation technique, they are therefore more sensitive to the anomaly types generated in the artificial process sample. Finally they are relatively simple methods, which require only limited user-input for the tuning of involved parameters and therefore might require less expert knowledge of the process and the detection technique in a future practical usage. Each of the discussed techniques assigns an anomaly score to every instance in the data sample, which is used to identify the anomalous sequences. In the following sections, the used techniques are discussed in detail.

6.1 Windows Based Method

For the windows based technique, a sliding window is used to extract subsequences of fixed length l from all process instances. All possible subsequences in the dataset are then, together with their frequency of occurrence, written in a normal dictionary. In a second iteration of the data sample, each subsequences with length l is assigned an anomaly score which is the inverse of the frequency associated with the same subsequence in the normal dictionary. Similar techniques have been proposed for intrusion detection [25] where for example the window is counted as anomaly in case the frequency is above a certain threshold (t-STIDE). The disadvantage of this method is that the threshold is another parameter in addition to the windows length l that needs to be defined. By using the inverse frequency as anomaly score for all possible subsequences this problem is avoided. In a last step, the anomaly score of the full sequence A_s is calculated as the sum of the anomaly scores of the subsequences a_s divided by the number of l length windows n_{win} in the sequence [26]:

$$A_s = \frac{\sum a_s}{n_{win}}. \tag{1}$$

6.2 Markovian Based Method

The Markovian based method estimates the conditional probability of an activity s_i in a sequence $S = (s_1, \ldots, s_n)$ based on the previous activities in the sequence. It basically relies on a higher order Markov condition, assuming that the probability for an activity s_i only depends on the previous l activities [27], i.e.:

$$P(s_i|s_1 \ldots s_{i-1}) = P(s_i|s_{i-l} \ldots s_{i-1}) \text{ for } l > 1. \tag{2}$$

Technically, a sliding window is used to extract all subsequences of length l and $l-1$ from the data set. Their frequency of occurrence is stored in a normal dictionary. In a second iteration, the conditional probability of each activity in a sequence is calculated as the ratio between the frequency of the subsequences $(s_{i-l}, .., s_i)$ and $(s_{i-l}, \ldots, s_{i-1})$:

$$P(s_i|s_1 \ldots s_{i-1}) = \frac{f(s_{i-l}, \ldots, s_i)}{f(s_{i-l}, \ldots, s_{i-1})}. \tag{3}$$

The conditional probabilities of the single activities s_i are combined to a total probability [23]:

$$P(S) = \prod P(s_i|s_1 \ldots s_{i-1}). \tag{4}$$

To consider the different length of the full sequences, the total probability is normalized to the number of l length windows n_{win} in a sequence and the anomaly score is set to

$$A_s = \frac{1 - P(S)}{n_{win}}. \tag{5}$$

A higher anomaly score then represents a higher probability for a sequence to be anomalous. A similar approach was proposed in [18].

6.3 Hidden Markov Model

In this method a Hidden Markov Model [28] is constructed which allows to transform the observed activity sequences in the data sample in sequences of n_s hidden states. The Expectation Maximization algorithm is used to perform a maximum likelihood fit to the data sample and determine the parameters of the Hidden Markov Model for the given set of hidden states. These parameters are the transition matrix, containing the transition probabilities between the hidden states, and the emission matrix with the output probabilities of the hidden to the observed activity states. After constructing the Hidden Markov Model, the Viterbi algorithm [29] is used to determine the most probable sequence of hidden states for each individual sequence in the data sample. Finally the windows based method as discussed previously is applied to the hidden sequences and

a corresponding anomaly score is assigned to each sequence. Similar approaches have been used in other research domains for anomaly detection [23].

7 Results

The windows based, Markov based and HMM based techniques are applied to the artificial process data sample. Each technique is applied four times, following the different sequential approaches discussed previously: First, only the activity sequence is analyzed in a one-dimensional way, i.e. sequences of the type *"Create Order"* - *"Check Customer Account"* -... (1d activity). Secondly, the person dimension is investigated, i.e. sequences like *"Sales/PersonA"* - *"Sales/PersonB"* -*"Sales/PersonB"* - *"Sales/PersonC"* -... (1d person). In a third approach, the one-dimensional person sequence is transformed such that consecutive identical persons are grouped together, i.e. *"Sales/PersonA"* - *"Sales/PersonB"* -*"Sales/PersonB"* -*"Sales/PersonC"* becomes *"Sales/PersonA"* - *"Sales/PersonB"* -*"Sales/PersonC"* (1d person merged). This approach tries to reflect possible situations in which the business process of a company is not split up in single activities but only contains information about the order of involved persons. Finally, in a multidimensional approach the activity and person information is combined. In this case a process event *"Create Order"* performed by *"Sales/PersonA"* is treated as different sequence element than the event *"Create Order"* performed by *"Sales/PersonB"* (2d activity-person), e.g. as *"Create Order | Sales/PersonA"* and *"Create Order | Sales/PersonB"*. Consequently, two otherwise identical process instances starting with these different elements would be counted as different.

In order to compare the performance of the different approaches, the process instances are ranked for each sequential detection technique in decreasing order according to the calculated anomaly score. With an optimal detection algorithm, all of the 259 anomalies in the sample would be at the top ranks of the anomaly score. In reality there are likely to be inaccuracies. As a performance measure to compare the different techniques, the number of detected true anomalies in the top ranked 259 instances is used. Table 1 shows the resulting number of detected anomalies for the different analysis approaches and detection techniques.

Table 1. Detected Anomalies with different analysis approaches

	1d activity	1d person	1d person merged	2d activity-person
Windows	171	221	184	253
Markovian	134	130	72	129
HMM	141	138	134	149

As discussed previously, the total number of anomalies in the sample is split up into 50% anomalies in the sequence, 40% anomalies in the person assignment and 10% in the overlap of both. The windows based method performs best for all the four approaches. Unsurprisingly, in the 1d activity case, the methods are only sensitive to

the anomalies in the activity sequence and hence the number of detected anomalies is limited to this type. For the 1d person approach the situation is a bit different. Especially the windows based method detects significantly more anomalies than only the ones affecting the person assignment. This can be explained by the fact that both a wrong assignment of a person, as well as a wrong activity sequence can change the person sequence. Interestingly, the other detection techniques are not able to gain in performance by picking up the different anomaly types with this approach. Also in the 1d person merged approach the windows based method detects a reasonable fraction of the anomalies but loses accuracy compared to the 1d person approach. This could be explained by the loss of information that comes with the merging of the consecutive identical person assignments. The two-dimensional approach gives by far the best performance for the windows based method. Almost all anomalies in the sample are detected. The other techniques again seem not to profit from the two-dimensional information view.

8 Interpretation of Results

The results obtained with the different analysis approaches on the artificial data sample show that the usability of sequential detection techniques is not only restricted to the activity sequence. In fact, performing the anomaly detection analysis on other dimensions, in the presented example the acting persons, can give additional insights. In case of correlations between different dimensions, performing a one-dimensional sequential analysis might even be sensitive to anomalies occurring in the sequence of another data dimension. In the presented example, the correlation between executed activities and responsible persons allowed to also detect anomalies in the activity sequence when analyzing solely the sequence of acting persons.

Furthermore, a simple combination of the information from two dimensions offers the possibility to use sequential techniques and detect anomalies appearing in both dimensions. In the presented example, it was differentiated between activities that are performed by different persons. Technically this can be achieved by a simple relabeling of the sequence element. A practical example where the two dimensional approach would be beneficial, is the case when one person (e.g.*"Logistics/PersonD"*) is in vacation and another employee (*"Purchase/PersonE"*) with less knowledge in this domain takes over the tasks but performs either the wrong activity or the correct activity in a wrong way (e.g. sending the wrong goods). Both cases would be recognized by the two-dimensional approach as the appearance of an employee in the wrong place of the process instance would be detected as anomaly.

This concept is of course not restricted to two dimension but can be applied to multiple dimension. In this case the sequential analysis becomes in principle sensitive to anomalies present in all involved data dimensions. For processes with high complexity in the data structure, e.g. many different activities that can be performed by multiple persons in various organization units, this concept however might not be practical. In this case, many differentiations would be necessary in the sequential analysis which would lead to a significant increase of the variety of normal sequences and therefore to a reduction of the separation power between normal and anomalous sequences.

The results from the example show as well that the sensitivity of the different analysis approaches can depend heavily on the chosen detection technique. The windows based method detects the most anomalies in all four analysis approaches. In fact this is the only method which is able to use the information from the person dimension to detect also anomalies in the sequence of executed activities (1d person and 1d person merged approaches). In addition it is also the method which profits most from the two-dimensional analysis approach in the presented example. The Markov and HMM methods on the other hand do not seem to profit from the additional information available. At least when considering the total number of detected anomalies both techniques do not perform much different in the two approaches. The presented results however show only the total number of detected anomalies, not separated according to their appearance in the activity or person sequence. To understand the qualitative difference between the windows based method and the Markov an HMM based methods, a performance study separated for the anomaly types must be performed as a next step in this research.

In this context, it is also important to note that the presented results correspond only to the specific choice of parameter settings for the different techniques, i.e. windows size, number of previous activities and number of hidden states. Although a few parameter settings were investigated and showed no significant difference in the final results, it might be possible that when carefully tuning the techniques, a better performance can be reached in some of the analysis approaches. In addition, the simulated business process is rather simple and real-world processes can be much more complex, in terms of possible process executions and also in the types of the anomalies. Therefore the presented comparison cannot be seen as universally valid but must only be interpreted as first insights in the usability of sequential techniques for one- and multidimensional analysis of business process data.

9 Summary and Conclusion

The availability of transactional data from information system allows for data-driven analyses and detection of anomalies in the business processes of a company. Anomalies can occur in different dimensions of the business process. Most of the existing research concentrates on the detection of anomalies in the sequence of the executed activities. In the presented paper, different approaches were investigated to use sequential techniques also for the detection of anomalies in other dimensions of the process data. In addition a simple concept of using multiple dimensions of process information was presented. The approaches were tested with three basic sequential detection techniques, a windows based, a Markov based and a Hidden Markov Model based method. On a simulated process sample, it was shown that by performing the anomaly detection analysis on other dimensions one can gain additional insights in a wider set of anomaly types. The combination of multiple data dimensions in a sequential analysis offers the possibility to improve the total detection accuracy. From the used detection techniques, the windows based method provided the best performance on the artificial sample.

In the next steps of this research, it is necessary to understand the performance of the discussed sequential detection approaches separately for different types of anomalies

and the dependence of the detection techniques on the parameter tuning as well as on the type and complexity of the business process. Especially for more complex processes, future research could investigate the usability of more advanced multi-dimensional detection approaches such as artificial neural networks.

References

1. van der Aalst, W.M.P.: Process-aware information systems: lessons to be learned from process mining. Trans. Petri Nets Models Concurr. **II**, 1–26 (2009)
2. Van Der Aalst, W.M.P., De Medeiros, A.K.A.: Process mining and security: detecting anomalous process executions and checking process conformance. Electron. Notes Theor. Comput. Sci. **121**, 3–21 (2005)
3. van der Aalst, W.M.P.: Process Mining. Springer, Heidelberg (2011)
4. Bezerra, F., Wainer, J., Van Der Aalst, W.M.P.: Anomaly detection using process mining. Management **29**, 149–161 (2009)
5. Bezerra, F., Wainer, J.: Algorithms for anomaly detection of traces in logs of process aware information systems. Inf. Syst. **38**, 33–44 (2013)
6. Bezerra, F., Wainer, J.: A dynamic threshold algorithm for anomaly detection in logs of process aware systems. J. Inf. Data **3**, 316–331 (2012)
7. Armentano, M.G., Amandi, A.A.: Detection of sequences with anomalous behavior in a workflow process. In: Chen, Q., Hameurlain, A., Toumani, F., Wagner, R., Decker, H. (eds.) DEXA 2015. LNCS, vol. 9261, pp. 111–118. Springer, Heidelberg (2015). doi:10.1007/978-3-319-22849-5_8
8. Chandola, V., Banerjee, A., Kumar, V.: Anomaly detection: a survey. ACM Comput. Surv. **41**, 1–58 (2009)
9. Jagadeesh Chandra Bose, R.P., van der Aalst, W.M.P.: Process diagnostics using trace alignment: opportunities, issues, and challenges. Inf. Syst. **37**, 117–141 (2012)
10. West, J., Bhattacharya, M.: Intelligent financial fraud detection: a comprehensive review. Comput. Secur. **57**, 47–66 (2016)
11. Joudaki, H., Rashidian, A., Minaei-Bidgoli, B., Mahmoodi, M., Geraili, B., Nasiri, M., Arab, M.: Using data mining to detect health care fraud and abuse: a review of literature. Glob. J. Health Sci. **7**, 194–202 (2014)
12. Ahmed, M., Naser Mahmood, A., Hu, J.: A survey of network anomaly detection techniques. J. Netw. Comput. Appl. **60**, 19–31 (2016)
13. Bezerra, F., Wainer, J.: Anomaly detection algorithms in business process logs. In: ICEIS 2008 – Proceedings of 10th International Conference on Enterprise Information Systems, AIDSS, pp. 11–18 (2008)
14. Bezerra, F., Wainer, J.: Fraud detection in process aware systems. Int. J. Bus. Process Integr. Manag. **5**, 121 (2011)
15. Sarno, R., Sinaga, F.P.: Business process anomaly detection using ontology-based process modelling and multi-level class association rule learning. In: 2015 International Conference on Computer, Control, Informatics and its Applications (IC3INA), pp. 12–17. IEEE (2015)
16. Kang, B., Kim, D., Kang, S.H.: Real-time business process monitoring method for prediction of abnormal termination using KNNI-based LOF prediction. Expert Syst. Appl. **39**, 6061–6068 (2012)

17. Cabanillas, C., Ciccio, C., Mendling, J., Baumgrass, A.: Predictive task monitoring for business processes. In: Sadiq, S., Soffer, P., Völzer, H. (eds.) BPM 2014. LNCS, vol. 8659, pp. 424–432. Springer, Heidelberg (2014). doi:10.1007/978-3-319-10172-9_31
18. Gupta, N., Anand, K., Sureka, A.: Pariket: mining business process logs for root cause analysis of anomalous incidents. Databases Networked Inf. Syst. **8999**, 244–263 (2015)
19. Jalali, H., Baraani, A.: Process aware host-based intrusion detection model. Int. J. Commun. Networks Inf. Secur. **4**, 117–124 (2012)
20. Rogge-Solti, A.: Temporal anomaly detection in business processes, vol. 16, pp. 35–42 (2010)
21. Quan, L., Tian, G.: Outlier detection of business process based on support vector data description. In: Computing, Communication, Control, and Management, 2009, CCCM 2009. ISECS International Colloquium, vol. 2, pp. 571–574 (2009)
22. Accorsi, R., Wonnemann, C., Stocker, T.: Towards forensic data flow analysis of business process logs. In: 2011 Sixth International Conference on IT Security Incident Management and IT Forensics, pp. 3–20 (2011)
23. Chandola, V., Banerjee, A., Kumar, V.: Anomaly detection for discrete sequences - a survey. IEEE Trans. Knowl. Data Eng. **24**, 1–16 (2012)
24. Burattin, A., Sperduti, A.: PLG: a framework for the generation of business process models and their execution logs. In: Muehlen, M., Su, J. (eds.) BPM 2010. LNBIP, vol. 66, pp. 214–219. Springer, Heidelberg (2011). doi:10.1007/978-3-642-20511-8_20
25. Warrender, C., Forrest, S., Pearlmutter, B.: Detecting intrusions using system calls: alternative data models. In: 1999 IEEE Symposium on Security and Privacy, pp. 133–145 (1999)
26. Hofmeyr, S.A., Forrest, S., Somayaji, A.: Intrusion detection using sequences of system calls. J. Comput. Secur. **6**, 151–180 (1998)
27. Ron, D., Singer, Y., Tishby, N.: The power of amnesia: learning probabilistic automata with variable memory length. Mach. Learn. **25**, 117–149 (1997)
28. Rabiner, L., Juang, B.H.: An introduction to hidden Markov models. IEEE ASSP Mag. **3**, 4–16 (1986)
29. Forney, G.D.: The viterbi algorithm. Proc. IEEE **61**, 268–278 (1973)