A Novel Approach to Detect Anomalies in Business Process Event Logs Using Deep Learning Algorithm

M. Vijayakamal and D. Vasumathi

Abstract Enterprises whose businesses are driven by web-based or cloud-based applications contain thousands of business processes involved. Due to the dynamic runtime environments and distributed nature of business processes and dependencies, there is possibility of noise and anomalies. Moreover, naturally, businesses are interested in finding anomalies in business processes and rectify them for improving quality of service (QoS). Especially, as part of process mining, anomaly detection has become an important research area in the contemporary era. Many anomaly detection methods came into existence based on machine learning techniques. There are attempts made using autoencoders for business process anomaly detection. However, from the literature, it is understood that there is need for a deep learning-based autoencoder with unsupervised learning approach for efficient detection of anomalies by analysing business process event logs. Towards this end, in this paper, we proposed a methodology and defined an algorithm known as deep learning encoder-based anomaly detection (DLE-AD) for enhancing the ability of anomaly detection. From the experiments, it is revealed that deep learning-based anomaly detection showed better performance over the traditional approaches. The proposed algorithm is evaluated against state of the art and found that it outperforms the existing methods.

Keywords Business process · Event logs · Process anomaly detection · Deep learning · Autoencoding

M. Vijayakamal (✉)
Research Scholar, Jawaharlal Nehru Technological University Hyderabad, Hyderabad, India

D. Vasumathi
Professor, Department of CSE, JNTUHCEH, JNTU Hyderabad, Hyderabad, Telangana, India

V. S. Reddy et al. (eds.), *Soft Computing and Signal Processing*, Advances in Intelligent Systems and Computing 1340, https://doi.org/10.1007/978-981-16-1249-7_34

1 Introduction

Business intelligence (BI) is given paramount importance by enterprises in every aspect of their business. Traditionally, machine learning methods are used for detection of anomalies in different applications. In fact, anomaly detection became an integral part of BI. It is more so in the context of process mining. Process aware information systems (PAIS) are emerged in the contemporary era. There has been increasing number of such systems where process mining plays vital role [1]. Different methods such as support vector machine (SVM) came into existence for anomaly detection. However, these techniques are supervised learning-based methods. It is not suitable for business processes, as they are highly dynamic in nature and evolving from time to time. Therefore, it is essential to have unsupervised learning-based methods for better performance.

Autoencoders have really attracted researchers and academia for detecting anomalies from business process event logs. It is reflected in the research carried out in [1, 6, 17, 18]. The autoencoding process using unsupervised learning method with deep learning is explored in [1] in presence of noisy business processes. In [16], business process event logs are used for anomaly detection using deep learning-based approaches. Similarly, in [17], temporal anomaly detection method is employed where time-related anomalies are found from business processes. In [18], on the other hand BINet, a multi-perspective classification method for anomaly detection is employed. From the literature, it is understood that there is need for an effective deep learning-based autoencoder for detection of anomalies from business process event logs. Our contributions in this paper are as follows.

1. A methodology is proposed for deep learning-based autoencoder for detection of anomalies from business process event logs.
2. An algorithm known as deep learning encoder-based anomaly detection (DLE-AD) is proposed to achieve the desired results.
3. An application is built to evaluate the proposed algorithm. The results are compared with existing methods. It is found that DLE-AD outperforms the state of the art.

The remainder of the paper is structured as follows. Section 2 reviews literature pertaining to deep learning-based methods for anomaly detection. Section 3 presents the proposed methodology for anomaly detection. Section 4 presents experimental results and evaluates the proposed method by comparing with existing methods. Section 5 concludes the paper gives directions for future work.

2 Literature Survey

This section reviews related literature on deep learning-based business process anomaly detection. Nolle et al. [1] considered noisy business process event logs and used unsupervised approaches for anomaly detection. They employed BPMN model for visual representation of processes. They employed deep learning-based autoencoder to detect anomalies. Kiran et al. [2] also used deep learning-based solution for anomaly detection, but it was for videos. Chong and Tay [3] proposed an autoencoder based on deep learning method. It is meant for abnormal events in the videos. The kind of autoencoder they used is known as spatiotemporal autoencoder. It is used for both quantitative and qualitative analysis. Suh et al. [4] proposed conditional variational autoencoder for anomaly detection (CVAE). Their algorithm is named as echo-state CVAE, as it is based on echo-state network. Van et al. [5] studied deep learning-based method for anomaly detection for improving state of the art.

Bao et al. [6] investigated on deep learning-based anomaly detection. They proposed a framework with two step process for anomaly detection. They employed supervised learning model for the purpose. In future, they intended to use multi-label classification for anomaly detection. Park et al. [7] proposed a robot-based deep learning approach for anomaly detection. For this, they employed LSTM-based autoencoder. It showed least false alarms. Baur et al. [8] proposed deep autoencoding models for anomaly detection. Their models are equipped with deep representation learning for effectiveness. Yousefi-Azar et al. [9] proposed deep learning-based anomaly detection solution for cyber security. Erfani et al. [10] used machine learning algorithm like SVM and also deep learning models for anomaly detection. They found the significance of deep learning for effectiveness.

Nolle et al. [11] analysed business process log events in order to find anomalies. They employed autoencoders for this purpose. They found that deep learning-based autoencoding models are more efficient. Garg et al. [12] proposed a hybrid mode for anomaly detection. It is based on both deep learning and software defined network (SDN). They could identify suspicious flows. Liu et al. [13] used deep autoencoders to find anomalies. It could determine malicious insiders. Dairi et al. [14] employed deep learning-based anomaly detection. They employed unsupervised learning. Koizumi et al. [15] proposed an anomaly detection method based on deep learning. Bezerra and Wainer [16] used business process event logs for investigation of anomaly detection. Rogge-Solti and Kasneci [17] proposed a temporal anomaly detection method for business processes. Nolle et al. [18] proposed a methodology for multi-perspective anomaly detection of business processes. From the literature, it is understood that there is need for an effective deep learning-based autoencoder for detection of anomalies from business process event logs.

3 Deep Learning Model for Anomaly Detection

This section presents deep learning-based methodology along with algorithm known as deep learning autoencoder-based anomaly detection, and then, the results are compared with the SAE-AD and DLE-AD [19] and other existing methods found in [16–18].

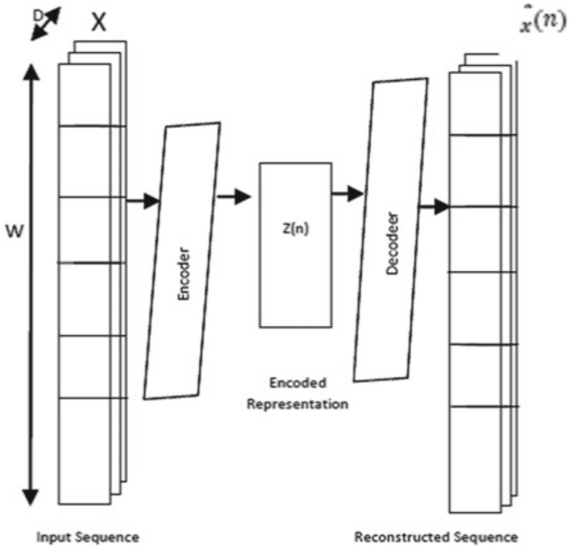

Fig. 1 Proposed architecture for deep learning-based LSTM approach

3.1 Methodology

Anomaly detection of business processes from event logs is carried out with deep learning approach. It is an autoencoding approach based on long short-term memory (LSTM) which is a deep artificial neural network architecture. It has feedback connections unlike feedforward neural networks. It is more efficient for dealing with time-series data. The long short-term memory—LSTM-based deep learning encoder-based anomaly detection (DLE-AD) algorithm is based on the architecture shown in Fig. 1.

As presented in Fig. 1, the LSTM-based approach is used for unsupervised learning as part of autoencoding. It is known as sequence to sequence autoencoder as the data used for processing is time-series based. It is meant for reconstructing sequences in order to identify anomalies. This is achieved by using an encoded representation of input sequence. The architecture is taught to learn with considered training samples with least reconstruction error.

3.2 Deep Learning Encoder-Based Anomaly Detection

An algorithm named deep learning encoder-based anomaly detection (DLE-AD) is proposed and implemented. It is based on the architecture presented in Fig. 1.

As presented in Algorithm 1, the algorithm takes the business process event log dataset and number of epochs as input. It detects anomalies and then enhances the processes where anomalies are found.

```
**Algorithm 6:** Deep Learning Encoder based Anomaly Detection
**Input:** Business process event log dataset D, maximum training epoch m
**Output:** Anomalies detected
$j \leftarrow 0$;
**while** $j < Epoch$ **do**
    **for each** process p in D **do**
        compute $h_T^{(m)} (m = 1, \ldots, M)$ on M sequences of aspect vectors;
        compute the process embedding $s_T$ by the attention model on M last hidden states;
        optimize the parameters based on the loss function
    **end**
    $j \leftarrow j + 1$;
detect anomalies
enhance process
**End**
```

Algorithm 1 Deep learning encoder-based anomaly detection

4 Experimental Results

4.1 Results

The observations of empirical study of DLE-AD algorithm are provided in terms of confusion matrix, reconstruction error and ROC curve.

As shown in Fig. 2, the confusion matrix with actual values or TP, FP, TN, FN for activity of all datasets is provided. For BPI-15 dataset, TP value is 15091, FP 122, FN 27834 and TN 4776. For BPI-16 dataset, TP value is 578, FP 2, FN 382 and TN 109. For BPI-17 dataset, TP value is 13468, FP 0, FN 8084 and TN 2448, while BPI-18 dataset shows TP value is 2574, FP 1, FN 2441 and TN 584.

The results revealed that the confusion matrix of each dataset is different from others due to dataset size and its dynamics.

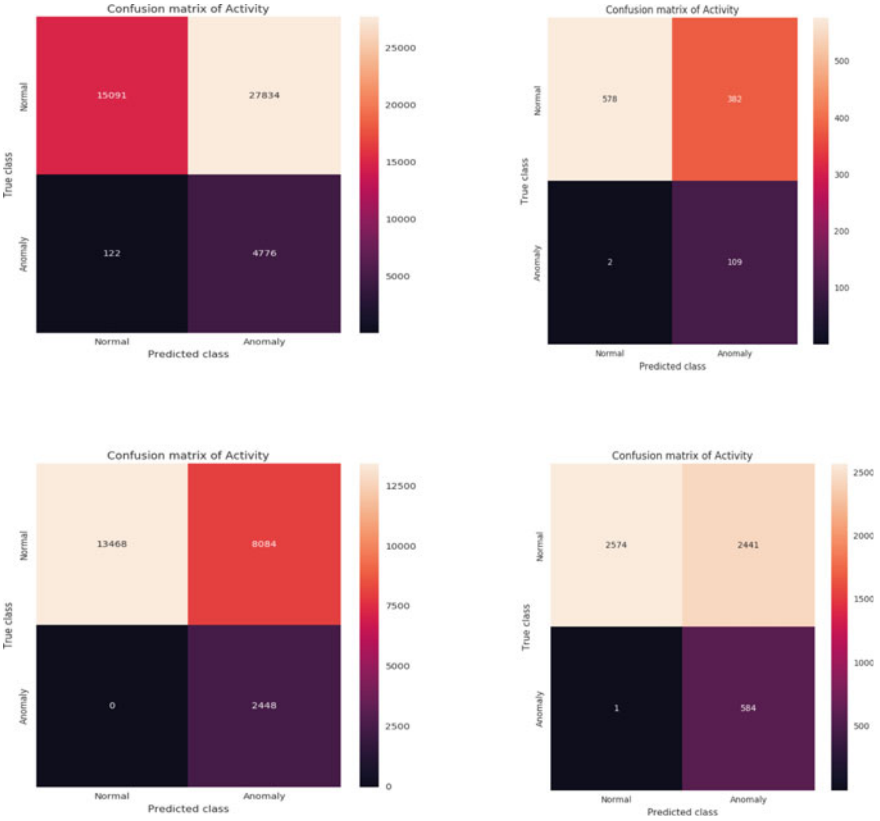

Fig. 2 Confusion matrix of DLE-AD for activity of four datasets (top left: BPI-15, top right: BPI-16, bottom left: BPI-17, bottom right: BPI-18)

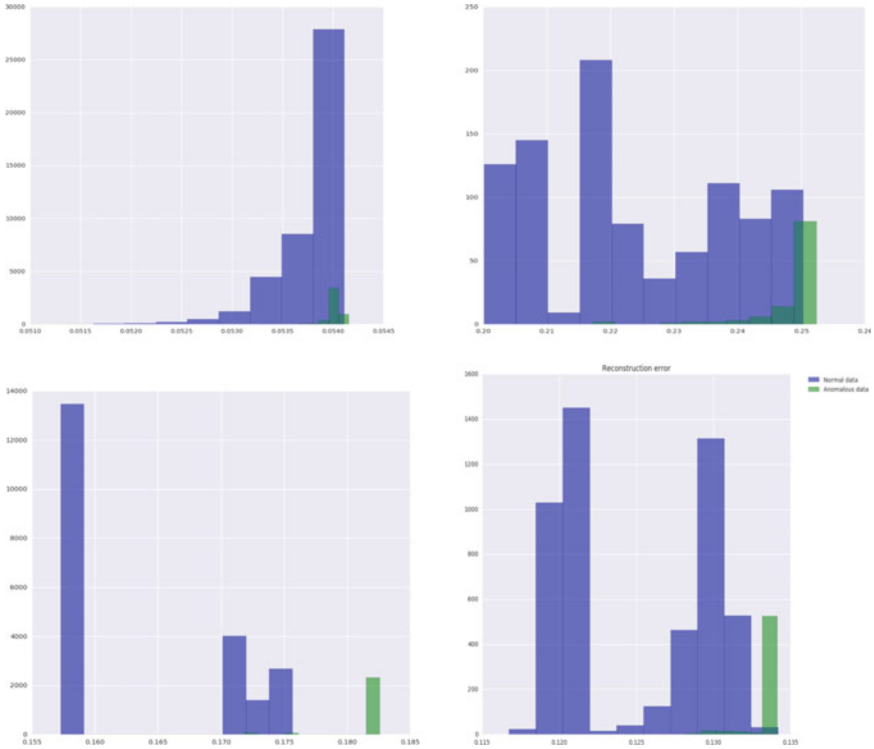

Fig. 3 Reconstruction error of DLE-AD for activity of four datasets (top left: BPI-15, top right: BPI-16, bottom left: BPI-17, bottom right: BPI-18)

As presented in the above Fig. 3, the reconstruction error is for normal cases and anomaly cases. The results revealed that the reconstruction error is computed and presented for BPI-15R, BPI-16, BPI-17 and BPI-18 datasets.

As presented in Fig. 4, ROC curve is plotted with false and true positives represented in horizontal and vertical axes, respectively.

AUC reflects the capability of proposed algorithm to distinguish abnormal log entries from that of normal ones.

The algorithm achieves 0.8892 for BPI-15 dataset, 0.9538 for BPI-16 dataset, 0.9919 for BPI-17 dataset and 0.9784 for BPI-18 dataset.

The results reflect significant capability of the algorithm in detecting anomalies.

4.2 Performance Evaluation

This section presents results of empirical study with different benchmark datasets. The results are compared with all the proposed methods and also state of the art.

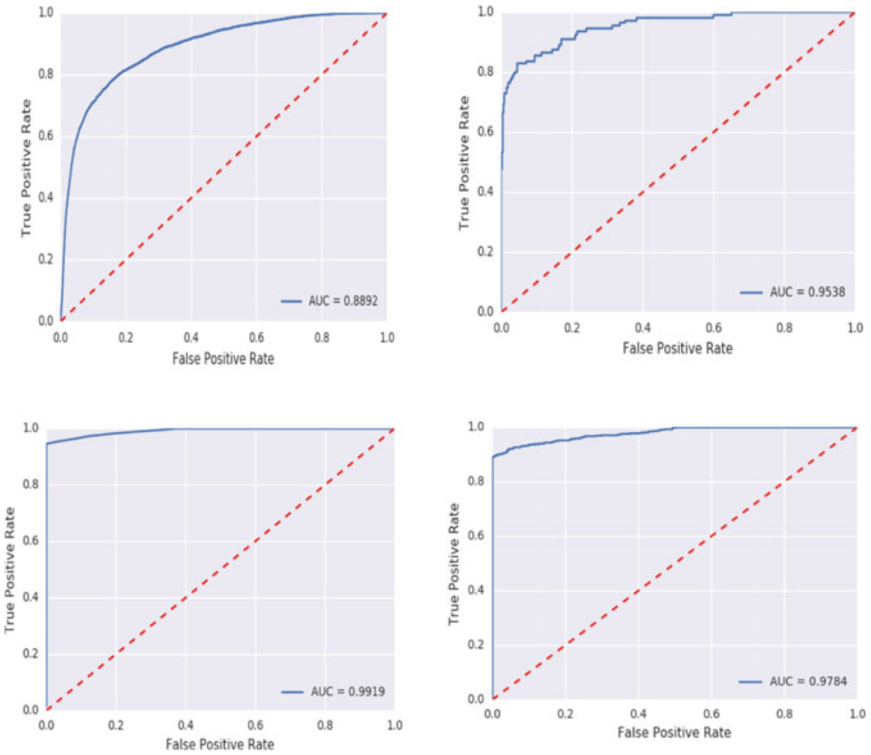

Fig. 4 ROC curve of DLE-AD for activity of four datasets (top left: BPI-15, top right: BPI-16, bottom left: BPI-17, bottom right: BPI-18)

As can be seen in Table 1, the results of the proposed method known as DLAE-AD are compared with other two methods in terms of precision, recall and F-measure for four datasets.

As can be seen in Fig. 5, different performance measures are provided in horizontal axis, while the vertical axis shows performance of the algorithms in terms of precision, recall and F-measure. Observations are made with four different datasets of business process intelligence (BPI) challenge. The results revealed that deep learning model outperformed the other two models. When F-measure is considered, the deep learning model showed highest performance for each dataset used.

As shown in Table 2, it is evident that that the proposed algorithms used for anomaly detection in business process event logs and enhancing processes are compared with the state-of-the-art algorithms.

As shown in Fig. 6, the experimental results of the proposed algorithms (SAE-AD, DLE-AD and DLAE-AD) are compared with the state-of-the-art algorithms found in the literature [16–18]. The results are observed for four datasets pertaining to BPI challenges. The existing and proposed methods are shown in horizontal axis, while the vertical axis shows the performance in terms of precision, recall and F-measure.

Table 1 Results of deep leaning-based approach compared with other methods

Methods	BPI 15			BPI 16			BPI 17			BPI 18		
	Precision	Recall	F-Measure	Precision	Recall	F-Measure	Precision	Recall	F-Measure	Precision	Recall	F-Measure
SAE-AD	0.99	0.56	0.72	0.99	0.69	0.81	0.99	0.97	0.98	1	0.88	0.94
DLE-AD	0.99	0.35	0.51	0.99	0.60	0.75	1	0.60	0.75	0.99	0.51	0.67
DLAE-AD	0.98	0.98	0.98	0.94	0.77	0.85	0.98	0.99	0.98	0.96	0.93	0.94

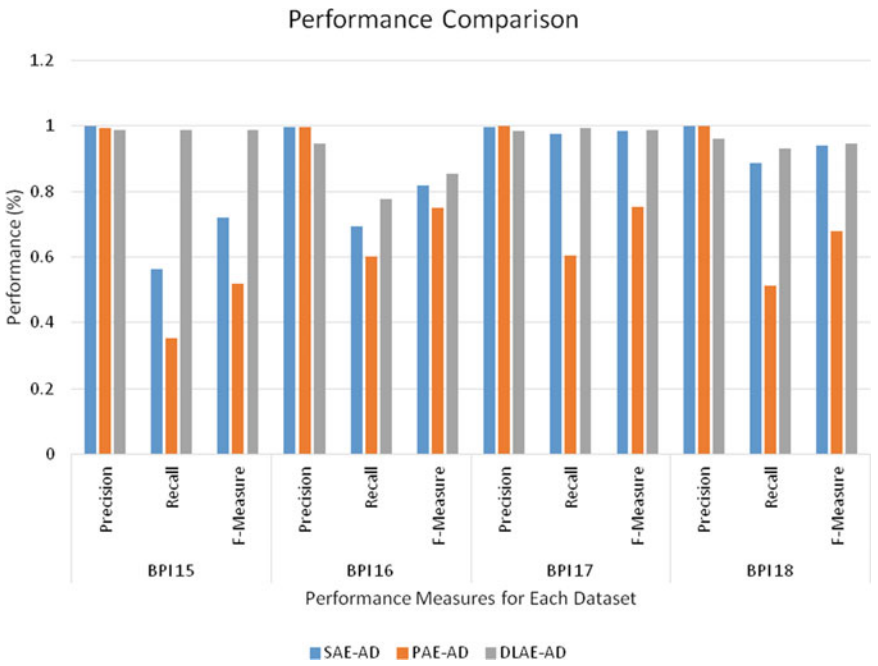

Fig. 5 Performance of DLAE-AD compared with other methods

Table 2 Performance comparison with the state of the art

Algorithm	BPI 15	BPI 16	BPI 17	BPI 18
Bezerra and Wainer [16]	0.65462	0.65042	0.62143	0.61323
Rogge-Solti and Kasneci [17]	0.70386	0.69324	0.72821	0.6321
Nolle et al. [18]	0.71284	0.72329	0.83423	0.685
SAE-AD	0.72032	0.818405	0.985404	0.94053
DLE-AD	0.519144	0.750614	0.753665	0.678261
DLAE-AD	0.895645	0.853253	0.98842	0.945711

From the results, it is understood that the deep learning-based approach used for detecting anomalies and enhancing processes showed better performance over the other proposed algorithms and also the state-of-the-art methods. At the same time, the three proposed algorithms showed better performance over the existing ones.

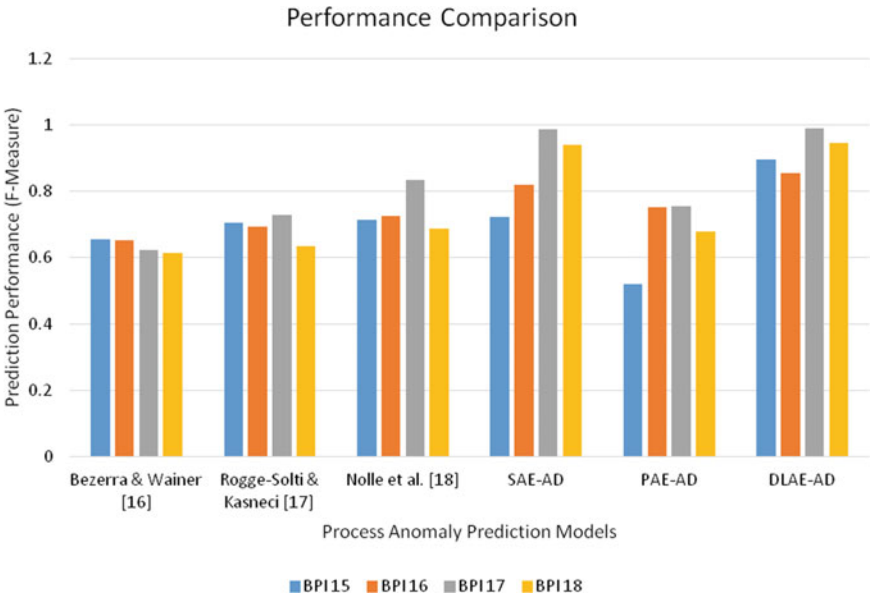

Fig. 6 Performance comparison against state of the art

5 Conclusion and Future Work

Business processes involved in an enterprise application are prone to have noise and also anomalies. When anomalies are not detected, it leads to deterioration of QoS. Therefore, enterprises are interested to find such anomalies to rectify them from time to time. The existing techniques based on deep learning are mostly employed in other domains. There is more research needed in the area of business process anomaly detection. Towards this end, in this paper, we proposed a methodology and defined an algorithm known as deep learning encoder-based anomaly detection (DLE-AD) for enhancing the ability of anomaly detection. From the experiments, it is revealed that deep learning-based anomaly detection showed better performance over the traditional approaches. The proposed algorithm is evaluated against state of the art such as SAE-AD and DLE-AD [19] and other existing methods found in [16–18] and found that it outperforms the existing methods. In future, we intend to improve our deep learning-based anomaly detection with a combination of autoencoding and convolutional neural network (CNN).

References

1. T. Nolle, A. Seeliger, M. Muhlhauser, *Unsupervised anomaly detection in noisy business process event logs using denoising autoencoders* (Springer International Publishing Switzerland, 2016), pp. 442–456
2. B.R. Kiran, D.M. Thomas, R. Parakkal, An overview of deep learning based methods for unsupervised and semi-supervised anomaly detection in videos. J. Imaging 1–25 (2018)
3. Y.S. Chong, Y.H. Tay, *Abnormal Event Detection in Videos Using Spatiotemporal Autoencoder* (Springer International Publishing AG, 2017), pp.189–196
4. S. Suh, D.H. Chae, H.-G. Kang, S. Choi, Echo-state conditional variational autoencoder for anomaly detection. Int. Joint Conf. Neural Netw. (IEEE, 2016) pp. 1015–1022
5. N.T. Van, T.N. Thinh, L.T. Sach, An anomaly-based network intrusion detection system using deep learning. Int. Conf. Syst. Sci. Eng. (IEEE, 2017), pp. 210–214
6. Y. Bao, Z. Tang, H. Li, Y. Zhang, Computer vision and deep learning–based data anomaly detection method for structural health monitoring. Struct. Health Monit. 1–21 (2018)
7. D. Park, Y. Hoshi, C.C. Kemp, A multimodal anomaly detector for robot-assisted feeding using an LSTM-based variational autoencoder. IEEE Robot. Autom. Lett. **3**(3), 1544–1551 (2018)
8. C. Baur, B. Wiestler, S. Albarqouni, N. Navab, *Deep Autoencoding Models for Unsupervised Anomaly Segmentation in Brain MR Images* (Springer Nature Switzerland AG, 2018), pp. 161–169
9. M. Yousefi-Azar, V. Varadharajan, L. Hamey, U. Tupakula, *Autoencoder-Based Feature Learning for Cyber Security Applications* (IEEE, 2017), pp. 3854–3861
10. S.M. Erfani, S. Rajasegarar, S. Karunasekera, C. Leckie, High-dimensional and large scale anomaly detection using a linear one-class SVM with deep learning. Pattern Recogn. **58**, 121–134 (Elsevier) (2016)
11. T. Nolle, S. Luettgen, A. Seeliger, M. Mühlhäuser, *Analyzing Business Process Anomalies Using Autoencoders* (Springer, Machine Learning, 2018), pp. 1–19
12. S. Garg, K. Kaur, N. Kumar, J.J.P.C. Rodrigues, *Hybrid Deep Learning-based Anomaly Detection Scheme for Suspicious Flow Detection in SDN: A Social Multimedia Perspective* (IEEE, 2018), pp. 1–13
13. L. Liu, O. De Vel, C. Chen, Anomaly-based insider threat detection using deep autoencoders. IEEE Int. Conf. Data Min. Workshops, 39–48 (2018)
14. A. Dairi, F. Harrou, M. Senouci, Y. Sun, Unsupervised obstacle detection in driving environments using deep-learning-based stereovision. Robot. Auton. Syst. 1–37 (2018)
15. Y. Koizumi, S. Saito, H. Uematsu, Y. Kawachi, N. Harada, Unsupervised detection of anomalous sound based on deep learning and the Neyman-Pearson Lemma. IEEE/ACM Trans. Audio, Speech Lang. Process. **27**(1), 212–224 (2019)
16. F. Bezerra, J. Wainer, Anomaly detection algorithms in business process logs, in *Proceedings of the Tenth International Conference on Enterprise Information Systems* (2008), pp. 11–18
17. A. Rogge-Solti, G. Kasneci, *Temporal Anomaly Detection in Business Processes*, pp. 1–16 (2010)
18. T. Nollea, S. Luettgen, A. Seeliger, M. Muhlhauser, BINet multi-perspective business process anomaly classification. Prepr. Submitted Inf. Syst. 1–25 (2019)
19. M. Vijayakamal, D. Vasumathi, Unsupervised learning methods for anomaly detection and log quality improvement using process event log. Int. J. Adv. Sci. Technol. 1109–1125 (2020)