# Convolutional and Long Short-Term Memory Recurrent Neural Network for Anomaly Types Classification

Jiechao Cheng, Rui Ren

[jetrobert19@gmail.com](mailto:jetrobert19@gmail.com), [renrui@ict.ac.cn](mailto:renrui@ict.ac.cn)

## Abstract

Anomaly detection and type classification problem for time series is a tedious but mush beneficial task, especially harnessing the massive amount of data generated by variable systems to create value for technology development and business strategies. By using the state-of-art machine learning techniques and deep neural networks, we propose a series of approaches to assist in focusing on detecting the most crucial types of anomalies and gaining critically insights of log information. Here we propose a state-of-the-art recurrent neural network approach and measure the accuracy of our diverse array of classification algorithms. The results reveal the strengths and advantages of our long short-term memory neural network and convolutional neural network for real-world classification tasks of anomaly types.

## 1 Introduction

Usually, log data is analyzed in order to detect misuses of a system or suspicious events indicating anomalies.

Anomaly discrimination related problems are addressed in a great deal of practical applications, including fraud detection, intrusion detection, system health monitoring as well as event detection in sensor networks. Anomalous items are also referred to as outliers, novelties, noise, deviations and exceptions [1].

In contrast to typical unsupervised anomaly detection, which is often applied on unlabeled data set under the assumption that the majority of the instances are normal, instead, we here take a data set that has been labeled as normal and abnormal into account for supervised anomaly classification tasks with the state-of-the-art deep learning algorithm classifier. In supervised learning, removing the anomalous data from the data set often results in a statistically significant increase in accuracy [2].

There are a diverse array of anomaly detection techniques have been proposed, such as density-based techniques [3, 4, 5], correlation-based outlier detection [6], cluster analysis-based outlier detection [7, 8] and ensemble techniques [9, 10]. When compared across huge data sets and hyper parameters, different methods have little systematic advantages over another in the measurement performance [11].

To classify types of anomalies at scale, we use different combinations of techniques starting with SVM and ending with CNN and LSTM sophisticated deep learning models.

The semantic transformation from a raw unstructured anomaly categorization task to a structured anomaly type classification task requires a solid background knowledge of the dataset, which features and instances are so different from the original raw data, namely the generation of a data view [12].

In fact, many practical anomaly detection problems often require a preprocessing in order to generate the appropriate data to handle with. The final step before the unsupervised anomaly detection algorithm can be applied is normalization. In practical applications, the min-max normalization is often used, every feature is normalized into a [0, 1] interval, so do we in the evaluation in this article

In this paper we present

## 2 Related Work

## 3 Algorithm

A label can be used as a result indicating whether an instance is an anomaly or not.

Let’s review discriminative algorithms from the perspective of application to finding various types of anomalies. The most suitable type of neural network working with time series is LSTM (Long Short-Term Memory) recurrent neural network, if properly built, it allows you to model the most sophisticated dependencies.

## 4 Experiments Settings

## 5 Results and Analysis

## 6 Conclusion

This area is still on-going research, and it requires a lot of work to build the model for the time series. Should you succeed, you may achieve outstanding performance results in terms of accuracy.

## Acknowledgments

## References

[1] Victoria J. Hodge, Jim Austin. A Survey of Outlier Detection Methodologies. Artificial Intelligence Review. 2004; 22(2):85-126. doi:10.1007/s10462-004-4304-y.

[2] Smith M. R., Martinez T. Improving classification accuracy by identifying and removing instances that should be misclassified. The 2011 International Joint Conference on Neural Networks. 2011; p. 2690. ISBN 978-1-4244-9635-8. doi:10.1109/IJCNN.2011.6033571.

[3] Knorr E. M., Ng R. T., Tucakov, V. Distance-based outliers: Algorithms and applications. The VLDB Journal the International Journal on Very Large Data Bases. 2000; 8(3-4):237-253. doi:10.1007/s007780050006.

[4] Breunig M. M., Kriegel H.-P., Ng R. T., Sander, J. LOF: Identifying Density-based Local Outliers. Proceedings of the 2000 ACM SIGMOD International Conference on Management of Data. SIGMOD. 2000; pp. 93–104. ISBN 1-58113-217-4. doi:10.1145/335191.335388.

[5] Schubert E., Zimek A., Kriegel H. P. Local outlier detection reconsidered: A generalized view on locality with applications to spatial, video, and network outlier detection. Data Mining and Knowledge Discovery. 2012; 28: 190–237.

doi:10.1007/s10618-012-0300-z.

[6] Kriegel H. P., Kroger P., Schubert E., Zimek A. Outlier Detection in Arbitrarily Oriented Subspaces. 2012 IEEE 12th International Conference on Data Mining. 2012; p.379. ISBN 978-1-4673-4649-8. doi:10.1109/ICDM.2012.21.

[7] He Z., Xu X., Deng S. Discovering cluster-based local outliers. Pattern Recognition Letters. 2003; 24(9-10):1641-1650. doi:10.1016/S0167-8655(03)00003-5.

[8] Campello R. J. G. B., Moulavi D., Zimek A., Sander J. Hierarchical Density Estimates for Data Clustering, Visualization, and Outlier Detection. ACM Transactions on Knowledge Discovery from Data. 2015; 10(1):5:1-51. doi:10.1145/2733381.

[9] Zimek A., Campello R. J. G. B., Sander J. R. Ensembles for unsupervised outlier detection. ACM SIGKDD Explorations Newsletter. 2014; 15:11–22. doi:10.1145/2594473.2594476.

[10] Zimek A., Campello R. J. G. B., Sander J. R. Data perturbation for outlier detection ensembles. Proceedings of the 26th International Conference on Scientific and Statistical Database Management-SSDBM. 2014; p.1. ISBN 978-1-4503-2722-0. doi:10.1145/2618243.2618257.

[11] Campos Guilherme O., Zimek Arthur, Sander Jörg, Campello Ricardo J. G. B., Micenková Barbora, Schubert Erich, Assent Ira, Houle Michael E. On the evaluation of unsupervised outlier detection: measures, datasets, and an empirical study. Data Mining and Knowledge Discovery. 2016; 30(4):891. ISSN 1384-5810. doi:10.1007/s10618-015-0444-8.

[12] Goldstein M. In: Markus Hofmann RK, editor. Anomaly Detection. Data Mining and Knowledge Discovery Series. Chapman and Hall/CRC. 2013; p.367-394.