Deep Learning for Anomaly Detection: Challenges, Methods, and Opportunities

Guansong Pang*
University of Adelaide
Adelaide, Australia
guansong.pang@adelaide.edu.au

Longbing Cao
University of Technology Sydney
Sydney, Australia
longbing.cao@uts.edu.au

Charu Aggarwal
IBM T. J. Watson Research Center
New York, United States
charu@us.ibm.com

ABSTRACT

In this tutorial we aim to present a comprehensive survey of the advances in deep learning techniques specifically designed for anomaly detection (*deep anomaly detection* for short). Deep learning has gained tremendous success in transforming many data mining and machine learning tasks, but popular deep learning techniques are inapplicable to anomaly detection due to some unique characteristics of anomalies, e.g., rarity, heterogeneity, boundless nature, and prohibitively high cost of collecting large-scale anomaly data. Through this tutorial, audiences would gain a systematic overview of this area, learn the key intuitions, objective functions, underlying assumptions, advantages and disadvantages of different categories of state-of-the-art deep anomaly detection methods, and recognize its broad real-world applicability in diverse domains. We also discuss what challenges the current deep anomaly detection methods can address and envision this area from multiple different perspectives.

Any audience who may be interested in deep learning, anomaly/outlier/novelty detection, out-of-distribution detection, representation learning with limited labeled data, and self-supervised representation learning would find it very helpful in attending this tutorial. Researchers and practitioners in finance, cybersecurity, healthcare would also find the tutorial helpful in practice.

CCS CONCEPTS

• **Computing methodologies** → **Anomaly detection**; **Neural networks**; *Scene anomaly detection*; • **Security and privacy** → *Intrusion/anomaly detection and malware mitigation.*

KEYWORDS

anomaly detection; deep learning; neural networks; outlier detection; representation learning; novelty detection

ACM Reference Format:
Guansong Pang, Longbing Cao, and Charu Aggarwal. 2021. Deep Learning for Anomaly Detection: Challenges, Methods, and Opportunities. In *Proceedings of the Fourteenth ACM International Conference on Web Search and Data Mining (WSDM '21), March 8–12, 2021, Virtual Event, Israel.* ACM, New York, NY, USA, 4 pages. https://doi.org/10.1145/3437963.3441659

*Corresponding to guansong.pang@adelaide.edu.au

WSDM '21, March 8–12, 2021, Virtual Event, Israel

ACM ISBN 978-1-4503-8297-7/21/03…$15.00
https://doi.org/10.1145/3437963.3441659

1 INTRODUCTION

Anomaly detection, a.k.a. outlier detection or novelty detection, can offer important insights into many safety-critical, commercially- or scientifically-significant real-world applications such as extreme climate event detection, mechanical fault detection, defect detection terrorist detection, fraud detection, malicious URL detection, just to name a few [2, 5]. Because of this significance, it has been extensively studied for decades, with numerous shallow methods proposed for this task [2, 5]. However, these methods are challenged by various data complexities, such as high dimensionality, data interdependency, data heterogeneity, etc [16]. In recent years deep learning has shown tremendous success in tackling these complexities in a wide range of applications, but popular deep learning techniques are inapplicable to anomaly detection due to some unique characteristics of anomalies, e.g., rarity, heterogeneity, boundless nature, and prohibitively high cost of collecting large-scale anomaly data. A large number of studies therefore have been dedicated to designing deep learning techniques specifically designed for anomaly detection. These studies demonstrate great success in addressing some major challenges to which shallow anomaly detection methods fail in different application contexts.

In this tutorial we aim to present a comprehensive review of the advances in deep learning-based anomaly detection. Through this tutorial, we present a systematic overview of this area by introducing the key intuitions, objective functions, underlying assumptions, advantages and disadvantages of different categories of state-of-the-art deep anomaly detection methods. This is to promote the recognition of the broad real-world applicability of deep anomaly detection in various critical domains. Further, deep anomaly detection is significantly less explored than many other data mining tasks. There are still many largely unsolved challenges in this area. Thus, we also aim to actively promote its development in algorithms, theories and evaluation through this tutorial.

2 RELATED WORK

Anomaly detection has been a long-standing problem in various communities for decades. Similar to classification, clustering, and regression, anomaly detection is one of the most fundamental tasks in data mining [1, 9]. Recently deep learning-based anomaly detection has demonstrated tremendous success in tackle challenging issues in which shallow anomaly detection approaches fail. This brings a surge of new interest from the data mining and machine learning community to this research topic. This tutorial is built

upon our recently released survey on deep anomaly detection [16] and the outlier detection book [2].

There was a relevant tutorial in WSDM 2020 given by a LinkedIn team [25], having a similar title as ours, but that tutorial focuses more on deep anomaly detection applications at LinkedIn, covering mainly methods for sequential/time series data. This may lead to a biased overview of this increasingly important area. There is another relevant hands-on tutorial in KDD 2020 [4] that mainly focuses on autorencoder- and generative adversarial network (GAN)-based approaches for anomaly detection. By contrast, in our tutorial we aim at providing a thorough treatment of this area by systematically reviewing the research problems and challenges of the area, presenting a comprehensive review of existing popular techniques for different types of data (tabular data, image data, video data, graph data, sequence/time series data, etc.) in an unified taxonomy, and delineating a number of exciting future opportunities.

3 TUTORIAL OUTLINE

The tutorial includes the following three sections.

Opening Section. We present an introduction of the research problems and key applications

- *Introduction to anomaly detection.* This part presents the problem nature and challenges of anomaly detection, summarization of traditional approaches, and some largely unsolved research problems in this area.
- *Overview of deep learning for anomaly detection.* This part presents the research problems and main challenges of deep anomaly detection, and discusses the taxonomy of current deep anomaly detection techniques and key conceptual frameworks.
- *Key successful real-life applications of deep anomaly detection.* We present some exciting application showcases in a variety of critical domains such as cybersecurity, industrial inspection, finance, planetary exploration, etc.

Methodology Section. This section presents three high-level categories of methods and 11 fine-grained subcategories of methods. Thus, it is divided into three subsections, with each subsection discussing one high-level category of methods shown in Figure 1.

- *Methodology Part I: Deep learning as generic Feature extraction.* In this part we present how existing popular deep learning models can be directly leveraged to extract low-dimensional feature representations for downstream anomaly detection. Some representative studies include unmasking [12], unsupervised classification approach [11], and adapted one-class SVMs [26].
- *Methodology Part II: Learning representations of normality.* We introduce key intuitions, objective functions, advantages and disadvantages of a variety of methods in this category. This type of methods is arguably the most popular deep anomaly detection approach. To provide insightful discussions on this category, we further divide the methods into two groups and separately introduce them.
  - *Generic normality feature learning.* We present methods that learn the representations of data points by optimizing a generic feature learning objective function that is not primarily designed for anomaly detection, but the learned representations can still well empower anomaly detection. This group of methods include autoencoder, generative adversarial networks, predictability modeling, and self-supervised classification approaches. Some representative algorithms include replicator neural network [10], RandNet [6], RDA [29], AnoGAN [22], ALAD [27], and GANomaly [3].
  - *Anomaly measure-dependent feature learning.* In this part we review methods that learn feature representations that are specifically optimized for one particular existing anomaly measure, including distance-based measure, one-class classification measure, and clustering-based measure. Representative algorithms include REPEN [14], RDP [24], Deep SVDD [20], and DAGMM [30].
- *Methodology Part II: End-to-end anomaly score learning.* We present a group of methods that optimize anomaly scores in an end-to-end manner. This includes four types of approaches, i.e., ranking models (e.g., SDOR [19], PRO [17], MIL-AD [23], DPLAN [15]), prior-driven models (e.g., DevNet [18], IRL-ADU [13]), softmax likelihood models (e.g., APE and its extension [7, 8]), and end-to-end one-class classification models (e.g., ALOCC [21], OCAN [28]. The key intuitions, objective functions, advantages and disadvantages of each method in this category will be reviewed in detail.
- *Key methods in closely relevant areas.* Additionally, we review key methods in some closely related areas, including out-of-distribution detection, adversarial example detection, curiosity learning in reinforcement learning, to stimulate innovative solutions across the areas.

Conclusion Section This section summarizes the development of this area and discusses important future research opportunities.

- *Summarization of the advances in deep anomaly detection.* We present a summarization and comparison of the methods introduced in the methodology section to provide insights into the current development of this area. This includes the discussion of neural network architectures, loss functions, and deep learning tricks used in these methods.
- *Future opportunities.* We discuss a number of exciting opportunities that may be explored to further advance this area in different directions.

4 FORMAT AND DETAILED SCHEDULE

The tutorial is broken into three parts as follows.

(1) **Shallow anomaly detection vs deep anomaly detection (30 min)**
   - Problem nature and challenges of anomaly detection
   - Research problems in deep anomaly detection
   - Shallow anomaly detection vs. deep anomaly detection
   - Key applications of deep anomaly detection
   - Comprehensive taxonomy of existing deep anomaly detection techniques

(2) **Deep anomaly detection: Three principal approaches and beyond (110 min)**
   - Methodology I: Deep learning as simple feature extraction
   - Methodology II: Learning representations of normality
     - Generic normality feature learning

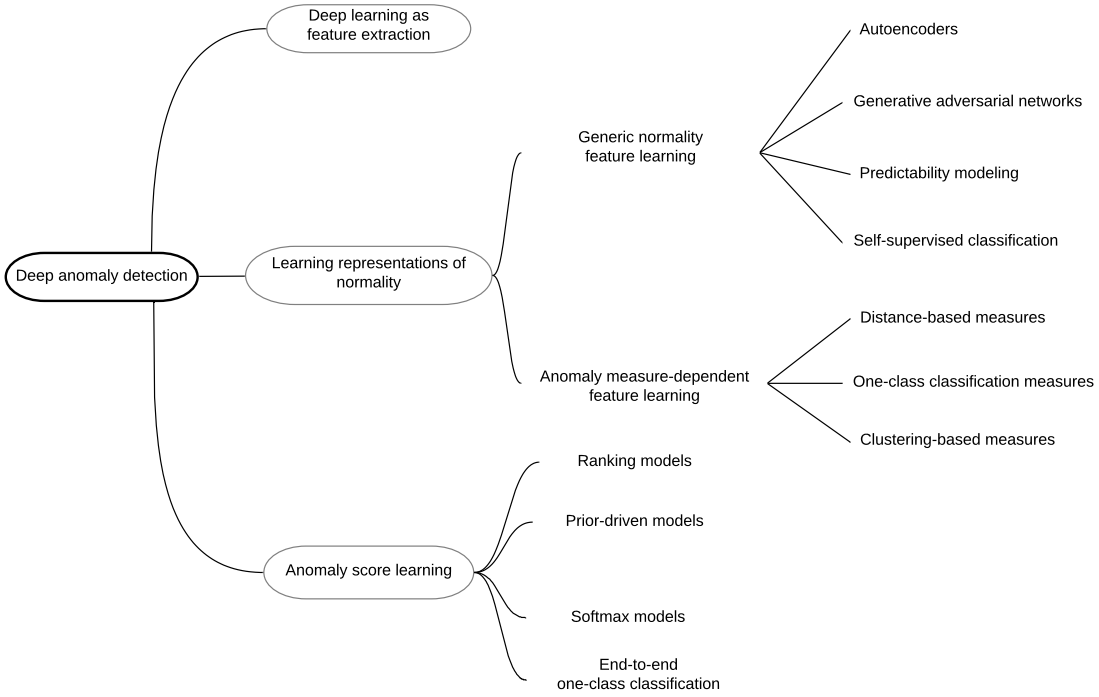

Figure 1: Taxonomy of Deep Anomaly Detection Methods [16]

    - Autoencoder-based approaches
    - Generative adversarial network-based approaches
    - Predictability modeling approaches
    - Self-supervised classification approaches
  - Anomaly measure-dependent feature learning
    - Feature learning for distance-based measure
    - Feature learning for one-class classification measure
    - Feature learning for clustering-based measure
- Methodology II: End-to-end anomaly score learning
  - Ranking models
  - Prior-driven models
  - Softmax models
  - End-to-end one-class classification models
- State-of-the-art methods in closely related areas
  - Out-of-distribution detection
  - Adversarial example detection
  - Curiosity learning in reinforcement learning

(3) **Conclusions and future opportunities (30 min)**

- Summarization of the advances in deep anomaly detection
- Future opportunities
  - Exploring new anomaly-supervisory signals
  - Deep weakly-supervised anomaly detection
  - Large-scale normality learning
  - Deep detection of complex anomalies
  - Interpretable and actionable deep anomaly detection
  - Novel applications and settings

In addition to embedded Q& A in each part above, there are 10 minutes for Q& A at the end of the tutorial.

5 TYPE OF SUPPORT MATERIALS TO BE SUPPLIED TO ATTENDEES

Self-contained slides will be provided to the attendees before the tutorial. Our survey paper [16] and book [2] will also be provided for the attendees to gain more in-depth understanding of this topic.

6 INTENDED AUDIENCE

This tutorial is designed for audience at all levels, covering from basic anomaly detection concepts and problems to advances in deep learning-based anomaly detection. While no specific knowledge is required from the audience, people who are familiar with anomaly detection or deep learning will find it more beneficial in understanding the algorithms and case studies to be introduced in this tutorial.

7 PRESENTERS

The tutorial is given by three presenters, including Guansong Pang, Longbing Cao, and Charu Aggarwal.

Dr. Guansong Pang (main contact) obtained his PhD degree in Data Mining at the University of Technology Sydney in 2019. He is a Research Fellow in the Australian Institute for Machine Learning at the University of Adelaide. His research interests lie in data mining, machine learning and their applications; he has been dedicating to the research on anomaly detection for over six years. He has published more than 25 papers (most of them are on (deep) anomaly detection) in refereed conferences and journals, such as KDD, AAAI, IJCAI, CVPR, ACM MM, ICDM, CIKM, IEEE Transactions on Knowledge and Data Engineering, and Data Mining

and Knowledge Discovery Journal. He is one of the key presenters of the KDD17's tutorial on "Non-IID Learning" and the KDD18's tutorial on "Behavior Analytics: Methods and Applications". He also gives a number of oral representations of his papers at top conferences such as IJCAI16, IJCAI17, CIKM17, KDD18, KDD19 and invited talks at various universities.

Prof. Longbing Cao has been a full professor in information technology at UTS since 2009. He is the founding Editor-in-Chief of Springer's Journal of Data Science and Analytics and associate EiC of IEEE Intelligent Systems. He serves as conference general chair such as for KDD2015, and program co-chair, area chair or vice-chair of conferences such as IJCAI, DSAA, PAKDD and ICDM, and SPC/PC member on over 100 conferences. He initiated and leads research on non-IID learning, behavior informatics, agent mining, and domain driven data mining, in addition to general issues in data science, data mining, machine learning, artificial intelligence and complex intelligent systems. He is one of the key presenters of a large number of tutorials at top conferences such as IJCAI 13, 19, 20; CIKM 14; KDD 17, 18; AAAI 18, 19; PAKDD 15, 18.

Dr. Charu Aggarwal completed his Ph.D. in Operations Research from the Massachusetts Institute of Technology in 1996. He has worked extensively in the field of data mining, with particular interests in data streams, privacy, uncertain data and social network analysis. He is a recipient of the IEEE ICDM Research Contributions Award (2015) and the ACM SIGKDD Innovation Award (2019), which are the two highest awards for research in the field of data mining. He has served as the general or program co-chair of the IEEE Big Data Conference (2014), the ICDM Conference (2015), the ACM CIKM Conference (2015), and the KDD Conference (2016). He is an editor-in-chief of the ACM Transactions on Knowledge Discovery and Data Mining , and has served as editor-in-chief of the ACM SIGKDD Explorations. He is a fellow of the IEEE (2010), ACM (2013), and the SIAM (2015) for "contributions to knowledge discovery and data mining algorithms". He is the sole author of the popular anomaly detection textbook "Outlier Analysis". He delivers a number of invited keynotes at various top conferences such as ECML 06, ASONAM 14, ECML 14 and SIGIR 18, and is one of the key presenters of several conference tutorials such as CIKM13 and SDM13 Tutorial on "Outlier Detection in Temporal Data" and ASONAM13 Tutorial on "Outlier Detection in Graph Data".

REFERENCES

[1] Charu C Aggarwal. 2015. *Data mining: the textbook.* Springer.

[2] Charu C Aggarwal. 2017. *Outlier analysis.* Springer.

[3] Samet Akcay, Amir Atapour-Abarghouei, and Toby P Breckon. 2018. GANomaly: Semi-supervised anomaly detection via adversarial training. In *ACCV*. Springer, 622–637.

[4] Raghavendra Chalapathy, Nguyen Lu Dang Khoa, and Sanjay Chawla. 2020. Robust Deep Learning Methods for Anomaly Detection. In *Proceedings of the 26th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining*. 3507–3508.

[5] Varun Chandola, Arindam Banerjee, and Vipin Kumar. 2009. Anomaly detection: A survey. *Comput. Surveys* 41, 3 (2009), 15.

[6] Jinghui Chen, Saket Sathe, Charu Aggarwal, and Deepak Turaga. 2017. Outlier detection with autoencoder ensembles. In *SDM*. 90–98.

[7] Ting Chen, Lu-An Tang, Yizhou Sun, Zhengzhang Chen, and Kai Zhang. 2016. Entity embedding-based anomaly detection for heterogeneous categorical events. In *IJCAI*. 1396–1403.

[8] Shaohua Fan, Chuan Shi, and Xiao Wang. 2018. Abnormal event detection via heterogeneous information network embedding. In *CIKM*. 1483–1486.

[9] Jiawei Han, Jian Pei, and Micheline Kamber. 2011. *Data mining: concepts and techniques.* Elsevier.

[10] Simon Hawkins, Hongxing He, Graham Williams, and Rohan Baxter. 2002. Outlier detection using replicator neural networks. In *DaWaK*.

[11] Radu Tudor Ionescu, Fahad Shahbaz Khan, Mariana-Iuliana Georgescu, and Ling Shao. 2019. Object-centric auto-encoders and dummy anomalies for abnormal event detection in video. In *CVPR*. 7842–7851.

[12] Radu Tudor Ionescu, Sorina Smeureanu, Bogdan Alexe, and Marius Popescu. 2017. Unmasking the abnormal events in video. In *ICCV*. 2895–2903.

[13] Min-hwan Oh and Garud Iyengar. 2019. Sequential Anomaly Detection using Inverse Reinforcement Learning. In *KDD*. 1480–1490.

[14] Guansong Pang, Longbing Cao, Ling Chen, and Huan Liu. 2018. Learning Representations of Ultrahigh-dimensional Data for Random Distance-based Outlier Detection. In *KDD*. 2041–2050.

[15] Guansong Pang, Anton van den Hengel, Chunhua Shen, and Longbing Cao. 2020. Deep Reinforcement Learning for Unknown Anomaly Detection. *arXiv preprint arXiv:2009.06847* (2020).

[16] Guansong Pang, Chunhua Shen, Longbing Cao, and Anton van den Hengel. 2020. Deep learning for anomaly detection: A review. *arXiv preprint arXiv:2007.02500* (2020).

[17] Guansong Pang, Chunhua Shen, Huidong Jin, and Anton van den Hengel. 2019. Deep Weakly-supervised Anomaly Detection. *arXiv preprint:1910.13601* (2019).

[18] Guansong Pang, Chunhua Shen, and Anton van den Hengel. 2019. Deep Anomaly Detection with Deviation Networks. In *KDD*. 353–362.

[19] Guansong Pang, Cheng Yan, Chunhua Shen, Anton van den Hengel, and Xiao Bai. 2020. Self-trained Deep Ordinal Regression for End-to-End Video Anomaly Detection. In *CVPR*. 12173–12182.

[20] Lukas Ruff, Nico Görnitz, Lucas Deecke, Shoaib Ahmed Siddiqui, Robert Vandermeulen, Alexander Binder, Emmanuel Müller, and Marius Kloft. 2018. Deep one-class classification. In *ICML*. 4390–4399.

[21] Mohammad Sabokrou, Mohammad Khalooei, Mahmood Fathy, and Ehsan Adeli. 2018. Adversarially learned one-class classifier for novelty detection. In *CVPR*. 3379–3388.

[22] Thomas Schlegl, Philipp Seeböck, Sebastian M Waldstein, Ursula Schmidt-Erfurth, and Georg Langs. 2017. Unsupervised anomaly detection with generative adversarial networks to guide marker discovery. In *IPMI*. Springer, Cham, 146–157.

[23] Waqas Sultani, Chen Chen, and Mubarak Shah. 2018. Real-world anomaly detection in surveillance videos. In *CVPR*. 6479–6488.

[24] Hu Wang, Guansong Pang, Chunhua Shen, and Congbo Ma. 2020. Unsupervised Representation Learning by Predicting Random Distances. In *IJCAI*.

[25] Ruoying Wang, Kexin Nie, Tie Wang, Yang Yang, and Bo Long. 2020. Deep Learning for Anomaly Detection. In *Proceedings of the 13th International Conference on Web Search and Data Mining*. 894–896.

[26] Dan Xu, Elisa Ricci, Yan Yan, Jingkuan Song, and Nicu Sebe. 2015. Learning Deep Representations of Appearance and Motion for Anomalous Event Detection. In *BMVC*.

[27] Houssam Zenati, Manon Romain, Chuan-Sheng Foo, Bruno Lecouat, and Vijay Chandrasekhar. 2018. Adversarially learned anomaly detection. In *ICDM*. IEEE, 727–736.

[28] Panpan Zheng, Shuhan Yuan, Xintao Wu, Jun Li, and Aidong Lu. 2019. One-class adversarial nets for fraud detection. In *AAAI*. 1286–1293.

[29] Chong Zhou and Randy C Paffenroth. 2017. Anomaly detection with robust deep autoencoders. In *KDD*. ACM, 665–674.

[30] Bo Zong, Qi Song, Martin Renqiang Min, Wei Cheng, Cristian Lumezanu, Daeki Cho, and Haifeng Chen. 2018. Deep autoencoding gaussian mixture model for unsupervised anomaly detection. In *ICLR*.