A Survey on Anomalies Detection Techniques and Measurement Methods

Gopinath Muruti
College of Computer Science and Information Technology,
Universiti Tenaga Nasional, Malaysia
Kajang Selangor
gopinathmuruti@gmail.com

Fiza Abdul Rahim
College of Computer Science and Information Technology,
Institute of Informatics and Computing in Energy (IICE),
Universiti Tenaga Nasional, Malaysia
Kajang, Selangor
fiza@uniten.edu.my

Zul-Azri bin Ibrahim
College of Computer Science and Information Technology,
Institute of Informatics and Computing in Energy (IICE),
Universiti Tenaga Nasional, Malaysia
Kajang, Selangor
zulazri@uniten.edu.my

***Abstract*—Dynamic research area has been applied and researched on anomaly detection in various domains. And various techniques have been proposed to identify unexpected items or events in datasets which differ from the norm. This review tries to provide a basic and structured overview of the anomaly detection techniques. Also, this review discusses major anomaly detection techniques using statistical based and machine learning based techniques. The outcome of this review may facilitate a better understanding of the different techniques in which research has been done on this topic by comparing the pros and cons of the identified techniques. In addition, this review also discusses on the measurement methods used by other researchers in validating their anomalies detection techniques.**

Keywords*—*anomalies detection, outlier detection, techniques, measurement, validation.

I. Introduction

Today the Anomalies in datasets produce by the current tools can happen by faults, glitches or cyber-attacks which require for anomaly detection techniques [1]. This activity to the task of searching patterns in data that does not fit in to usual behavior of the data [2].

Fig. 1 illustrates example of two-dimension anomalies, regions N_1 and N_2 represents area with normal data because the majority of observations are in these areas. While points $O_{1,}$ O_2, and area O_3 which are further away from normal areas are anomalies.

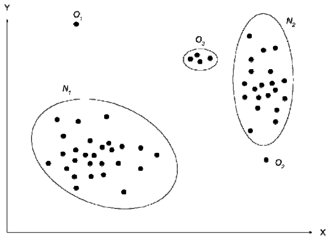

Fig. 1. Sample of Two-Dimension Anomalies

The term anomalies and outliers are two of the phrases which are frequently used sometimes interchangeably between each other in the field of anomaly detection [3]. Anomaly detection can be utilize in many usages of domains. As an example, in a network an anomalous traffic pattern could indicate that there is a malicious device or node in the network is vulnerable to cyber-attacks or have gone rogue [4]. An anomalous scan on electronic medical record could indicate the presence of disease outbreaks [5] or errors in the electronic medical records [6]. Anomalies in credit card transaction data could be utilized to show proof of credit card fraud [7].

Research on identifying anomalies or outliers has been extensively studied in the statistics society since the 19th century. As time goes by, various anomaly detection techniques have been created and a considerable lot of these techniques have been particularly created to suite certain application areas while others are more to nonspecific domains [8].

The paper is organized as follows. In Section II presents the related applications of anomaly detection. Section III presents the anomalies detection techniques classification. In Section IV, details review on anomalies detection techniques are discussed. Discussion on anomaly detection techniques measurement are summarized in Section V. Finally, conclusions and future works are given in Section VI.

II. Applications of Anomaly Detection

Anomaly modelling essentially depends on two things. The first is forming a behaviour profiles for the normal activities and present activities; and then these profiles are accorded in light of different techniques to identify any form of deviation from the normal behaviour [9]. Anomaly detection has wide range of applications in business, ranging from intrusion detection to health monitoring system and from credit card fraud detection to fault detection in critical information systems [10].

A. Intrusion Detection

Intrusion detection denotes to detection of malicious activities such as breach in a computer-based system. In the viewpoint of information security, these breaches are useful. A breach veers off from the standard system behaviour, and therefore anomaly detection techniques are deemed suitable for the domain of intrusion detection systems (IDS). According to [11], IDS can be classified into two categories which are network-based and host-based intrusion detection systems. Network-based IDS deal with intrusions that typically occur as anomaly in the network data. Through certain techniques, the network data is modelled in a sequential fashion to detect anomalous patterns [12]. However, the hurdle faced by anomaly detection techniques

978-1-5386-6925-9/18/$31.00 ©2018 IEEE

is related with the characteristics of anomalies as network attacks keeps evolving and adapting over time [13].

While host-based IDS deal with operating system traces. The intrusions are in the form on collective anomalies of the traces which translate to policy violations, malicious applications, and unapproved actions. Furthermore, host-based IDS require the anomaly detection techniques be able to handle sequential data since point anomaly detection technique is deemed not suitable for host-based IDS.

B. Fraud Detection

Fraud detection denotes to identification of unlawful activities that are happening within a business associations such as credit card companies, banks and insurance firms [14] , [15]. The malicious users could masquerade as a legitimate user of the services provided by the business organizations. The fraud happens when these users utilizes the provided resources in an unsanctioned manner. Hence, business organizations are keen to prioritize identification of such frauds in order to reduce monetary losses.

In the domain of credit card fraud identification, anomaly detection techniques are utilized to identify fraudulent transactions [16]. Credit card data is commonly comprised of records such as amount spent, user ID, and transaction duration [16]. The frauds are usually reflected as point anomalies in transactional records. It corresponds to high number items purchased or payments that have been never done by the user before. Clustering and profiling based techniques are commonly used by credit card companies to distinct data based on the credit card user since credit card companies have complete labelled data records [16].

C. Medical Anomaly Detection

In medical domain, anomaly detection included patient records. Data anomalies can occur in patient record due to recording errors, device error, or unusual patient condition [17]. Additionally, several anomaly detection techniques have been utilized in identifying disease outbreaks within a specific area [18]. Hence, anomaly detection in medical domain is vital and requires high degree of precision [6].

In this domain majority of the techniques focus on identifying point anomalies, and generally the data consists of patient weight, patient age, and blood group. Additionally, the techniques also handles time series data such as from Electrocardiograms (ECG) [19] collective anomaly detection techniques have been applied for recognizing anomalies in the data. However, the challenging portion is the cost involved in classifying an anomaly is costly.

III. Anomalies Detection Techniques Classification

Majority of the anomaly detection techniques utilize labels to identify whether the instance is normal or anomalous as final decision [20]. Obtaining a labelled data that is precise and represents a wide range of behaviours is expensive and difficult, Anomaly detection techniques can be categorized into three modes depending on the availability of the labels [21];

A. Supervised Anomaly Detection

Both abnormal and normal behaviours are modelled by using the supervised anomaly detection. It requires pre-labelled data classified as abnormal and normal in order to detect anomaly [22]. Multiple training models are utilized to identify the abnormal or normal data in the dataset [22]. Supervised techniques works by following these approaches; the training model is compared with dataset to identify anomalous data in dataset that has been classified as normal data and in opposite some of the anomalous data is then compared against the training model to find abnormal data [23].

B. Semi-Supervised Anomaly Detection

This category of technique assumes that the training data has labelled instances of the normal class while labels for the anomaly is not required. This category of technique is widely utilized than supervised technique. As an example, [24] utilized semi-supervised algorithm to detect anomalies in online social network.

C. Unsupervised Anomaly Detection

In unsupervised techniques, data set is only labelled with one label as normal. Training model detects abnormal class by itself from dataset. It works by using the clustering mechanism [25]. This technique finds cluster of nodes in which behaviour is similar to group. However, this assumption becomes wrong as many anomalies also make clusters with similar pattern. Unsupervised techniques are not efficient in producing accurate results and often suffer from high false positive rate [26].

IV. Anomaly Detection Techniques

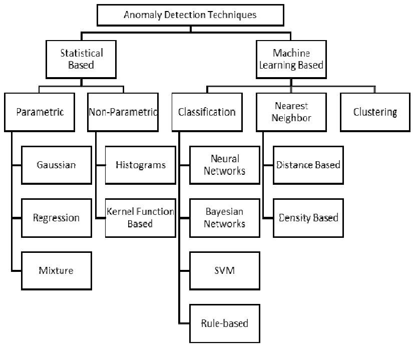

Fig. 2. Overview of Anomaly Detection Techniques

In this section, we review several techniques that have been proposed and used for anomaly detection. These include statistical based technique, and machine learning based technique as shown in Fig. 2.

A. Statistical Based Techniques

Statistical anomaly models primarily considers; the statistical measures such as the mean and standard deviation, the distribution of the data and the figured up probabilities for constructing the behaviour profiles [27]. Statistical tests are utilized to distinguish any sort of deviations of the present behaviour from the normal behaviour. In developing statistical anomaly detection models, non-parametric and parametric techniques is utilized [28]. Non-parametric techniques do not have the information of underlying distribution from the given data while parametric techniques have the information.

I. Parametric Techniques

In this technique, the normal data is assumed to be created by parameters and the score for the anomaly of data instance. Parametric techniques can be additionally classified as regression model based, Gaussian model based and mixture of models. In the regression model based, the data is set into a regression model and the residual of each data that is not highlighted by the model is measured. This is then considered to be the anomaly score of the instance.

The data is assumed to belong to Gaussian distribution in the Gaussian model based. The parameters of the model is premeditated by using maximum likelihood estimation of the data instances [29]. Tests such as the chi-square test can be utilized to decide whether a data instance is anomalous or not. While in mixture based models, hybrid of parametric models is used.

Multiple parametric based anomaly detection techniques have been applied in several past studies such as in [30]. Parametric based techniques were utilized to detect network anomalies in aggregate traffic by adopting simple statistical models for anomalous and background traffic in the time domain. They evaluated the technique by measuring the performance of the technique in various scenario and found the technique were able to detect all the network anomalies in all the scenarios within few seconds or less.

While in [31], a supervised and regression based anomaly detection model were used to identify anomalies in smart grid data. The model was then evaluated in terms of accuracy and scalability by using an experimental setup on real world electricity consumption data set. The results from the experimental setup shows that the model was able to provide an accurate detection rate of anomaly while having a good scalability to adapt with the huge volume of smart meter data.

Regression based analysis technique for anomaly detection in cloud operations were discussed in [32]. Experiments with various configurations with and without randomly injected faults to simulate failure of software and system in cloud virtual machines were conducted. The results of the experiment showed that the regression-based analysis technique was able to detect the injected faults with high accuracy and performance.

II. Non-Parametric Techniques

In non-Parametric techniques, normal data instances are used to generate a model, no model is assumed as deductive. The deviation of a given data from the model would assign the anomalous score [33]. In histogram-based models, histogram consisting of bins is produced from the estimations of the normal data. To decide, whether a given instance is anomalous or not, it gets plotted to check whether it falls in any of the histogram bins and in the event that it does falls into any one of the histogram bins, the instance is considered to be anomalous [34].

Meanwhile Kernel based modelling technique aims at deducing a similarity function based on the provided data allowing construction of model based on the data instances. And if the given data instances do not completely portray the specific behaviour, it lacks in terms of accuracy.

Non-parametric based techniques for detecting anomalies have been applied and studied in past studies for example in [35] a kernel based anomaly detection model to identify anomalous sequences. The researchers demonstrated the performance of the model by comparing with results of other tests on real world dataset. While in [36], a multi-scale non-parametric anomaly detection technique for video surveillance applications were discussed and studied. The technique was evaluated by comparing with other techniques in terms of detection rate and performance. The technique was found to have best performance with respect to another techniques when comparison was performed on publicly available data.

Meanwhile, a computationally efficient non-parametric method to detect persistent anomalies in high dimensional datasets were developed in [37]. The researchers justified the performance of their method based on numerical results from test on both simulated and real datasets. Similarly in [38], a non-parametric method for effectively detecting anomalies in large-scale systems were proposed. The researchers conducted experiments and compared their method with three commonly used detection methods which are; distance based (DB) approach, nearest neighbour (NN) approach and local outlier factor (LOF) based approach. The researchers demonstrated that their method able to provide high detection rate, accuracy and scalability in identifying the anomaly patterns.

III. Pro and Cons of Statistical Based Techniques

However, statistical based techniques are not truly prefect. It does have some pros and cons. The pros of statistical based techniques are, by off the chance that the presumptions in view of the data distribution is true, it can offer a statistically legitimate answer for anomaly detection. Additionally, the sureness level related to anomaly score can be applied as additional information for building a verdict.

B. Machine Learning Based Techniques

The major advantages machine learning based techniques is its ability to improve the capability of distinguishing anomalous behaviour from normal behaviour based on experience [39]. It adapts to unseen anomalies [40] . According to [41], machine learning based techniques categorizations are either classification, nearest-neighbour, and clustering.

I. Classification

The principle objective of classification-based technique is to assign each data instance to either one of the preset classes considering their features. Common examples include;

- Neural Networks, A neural network mimics the human nervous system and consist of a set of highly interconnected process which operates asynchronously with local data [42]. Normal data instances are utilized to train a neural network. And depending on the data label, neural networks works in both supervised and unsupervised learning [42].

- Bayesian Networks, is a graphical model which translates probabilistic connections among factors of interest [43]. It functions based on supervised learning. It operates by evaluating the posterior probability of an occasion given some precondition [43].
- Support Vector Machine (SVM), a supervised learning algorithm that plots the training data instances to a multi-dimensional plane [44]. The multi-dimensional plane gaps the data instances into two disjoint groups [44]. SVM are trained only with normal data, SVM is treated as a linear classifier due to the fact that it uses a borderline to gap the data instances into normal and anomalous [45].
- Rule-based, it is a supervised learning in which learns the rules which capture the normal behaviour of data instances. Therefore, if the rules fails to capture a data instance it is then the data instance is considered anomalous. Decision trees technique from the bunch of rule based techniques is utilized to study the rules via the training data instances [46].

Classification based techniques for detecting anomalies have been studied in past studies such as in [47] a unsupervised one-class SVM (OCSVM) model is used to detect anomalies in wireless sensor network (WSN) data. The model is evaluated in terms of detection rate and detection accuracy by conducting experiments on environmental sensor dataset collected from IBRL, LUCE, PDG, and NAMOS. The results from the experiments showed that the model had best performance and detection accuracy for the NAMOS dataset when compared to all schemes. While in [48], a fully convolutional neural network based method were utilized to identify anomalies in video data from surveillance cameras. The researchers evaluated the performance of the method based on UCSD and Subway benchmarks. It was found the method had better performance than other methods.

In [49], a rule based anomaly detection technique were proposed to detect anomalies in sensor data. The performance and detection accuracy of the technique were evaluated by comparing with current anomaly detection algorithms such as Gaussian, binary association rule and fuzzy association rule in which sensor data from various domains such as rainfall, temperature and cancer cell data were utilized. The comparison showed that the technique had more performance and accuracy in detecting anomalies. Meanwhile, in [50] a hybrid rule based anomaly detection technique were proposed to detect anomalies in online social network graphs. The proposed technique was applied to real world datasets from online social networks. The researchers showed that their technique had improved accuracy in comparison to existing techniques.

The pros of classification-based techniques are its ability to differentiate between multiple class via powerful algorithms and high efficiency of testing phase because each test data instances need to be compared with the precomputed model. However, the con of this technique is it relies upon on accurate and representative labels for different classes.

II. Nearest-neighbor

This technique utilizes either distance or density based functions to gauge the distance between a data instance to its nearest neighbour. The anomalous score of that instance is the distance. Depending on the data label, this technique can operate in unsupervised and supervised learning.

There are several nearest-neighbour based anomaly detection techniques that have been studied in past studies such as in [51] which presented a distance based nearest-neighbour method to detect anomalies in large scale traffic data. The method was evaluated both in unsupervised and semi-supervised approaches. The semi-supervised approach was found to have better accuracy in identifying anomalies. While in [52], a distance based outlier detection method using anti hubs were proposed to identify outliers in high dimension data. The proposed method was experimented with and without the anti-hubs on KDD datasets. The result of experiment showed that the method which used the anti-hubs had a better accuracy in detection.

Additionally in [53], isolation based anomaly detection using nearest-neighbour based mechanism were proposed to overcome the weakness of the previous isolation based mechanism. The mechanism was evaluated using local anomalies and anomalies in high dimension data. The evaluation results showed that the proposed mechanism was able to scale up with the increasing data set size and had a better performance in identifying the anomalies. A scalable distance based outlier detection method were proposed in [54] to detect anomalies in high volume data streams. The researchers evaluated the scalability and performance the proposed method by conducting experiments on real world streaming datasets and synthetic datasets. The results of the experiments showed that the proposed method had high scalability and performance in comparison to other techniques.

The pros of nearest neighbour-based techniques are it is widely adapted and does not need any distribution for the data and adapting it to various data type is straight-forward. However, the cons of this technique are that in the event that the normal data instances don’t have sufficiently do not have close neighbours or the anomalies have close neighbours, the technique can fail to label the anomalies. Additionally, the computing complexity involved in this technique is a challenge.

III. Clustering

Clustering based techniques utilizes unsupervised learning method works to recognize gatherings of identical training data instances. Anomalies might model a sparse cluster or does not fit in to any cluster at all. The cons of clustering based techniques are that it faster than distance based technique because it requires less computing complexity. However, the con of this technique is that it may not offer accurate insights in smaller data instances.

Various clustering based anomaly detection techniques have researched in past studies, for example in [55] cluster based anomaly detection technique is proposed to detect anomalies in smartphone applications. The researchers evaluated the detection accuracy of the proposed technique by testing on data set containing mixture of normal and abnormal applications. The experimental result showed that the proposed technique had detection accuracy in identifying abnormal applications. While in [56], a cluster based anomaly detection algorithm was proposed for healthcare data. Experiments was conducted to evaluate the proposed algorithm by testing on health care datasets. The results of the experiments showed that the proposed algorithm has better accuracy than distance-based anomaly detection method.

V. Discussion on Anomaly Detection Techniques Measurement

Regardless of the approach, anomaly detection begins with learning stage in which it gets presented with the training dataset. Once the learning phase have completed, it is ready to classify unseen instances and specific metrics that measures the performance gets calculated [57]. In a normal anomaly detection scenario, detecting anomalies accurately is vital, but not good enough [58]. In order to evaluate an anomaly detection technique, standard metrics such as detection rate, accuracy, performance and scalability metric were developed.

A. Detection Rate

Detection rate is a typically utilized metric to gauge an anomaly detection technique. In his research [59] has mentioned that the outcome of detection in anomalies detection rate can fall into four categories which are True Positive (TP), True Negative (TN), False Positive (FP) and False Negative (FN). The typically utilized metric in detection rate is the TP and TN in which defines the proportion of the instances categorized as anomalous by the detector. Meanwhile FP is another important metric which refers to the proportion of the instances being categorized wrongly as anomalous [59] as it can be triggered by meaningless activities. The FN rate is the proportion of the anomalous instances incorrectly categorized as normal [59] which can be fatal as these activities always been ignored. This metrics were utilized by researchers in [36], [38] and [47] to evaluate or measure their proposed anomaly detection techniques or methods.

B. Accuracy

Accuracy metric refers to the ratio of all correctly classified instances either normal or anomalous. The precision metric is the proportion of accurately grouped anomalies to all instances classified as anomalies. It was widely used by researchers in [31],[38],[49],[32],and [47] to evaluate or measure their proposed techniques. Additionally, this metric were also utilized by researchers in [50],[51],[52],[55] and [56] to gauge their developed techniques.

C. Performance

The receiver operating characteristics (ROC) metric is utilized to gauge the performance of the technique. It is created by plotting the TP rate against the FP rate at varying threshold values in which threshold acts as the cut-off point in determining an instance is anomalous or normal. This metric were widely used in [30],[35],[37],[32],and [36] to gauge the performance of the proposed technique or method. Additionally, it were also applied in studies [48],[49],[53],and [54].

D. Scalability

Scalability metric defines the ability for the anomaly detection technique to scale out and to efficiently cope with the increase in size of datasets. This metric were utilized by researchers in [31],[38],[53],and[54] to measure the scalability rate of their techniques to increasing dataset sizes. Different workload have to be tested to make sure that the technique can handle rapid changes of big data volume [31].

VI. Conclusions

In this paper, we have addressed various anomalies detection techniques through reviewing past literatures. Machine learning based anomaly detection techniques are the most widely used in identifying anomalies due to its capability of distinguishing anomalous behaviour from normal behaviour based on experience and adapts to previously unseen anomalies.

Our contribution also includes a comparison of various measurement methods that assists in finding the most relevant evaluation metrics. Accuracy and performance metric were found to be used most in gauging or measuring the anomaly detection techniques. Accuracy and performance metric provide a comprehensive evaluation of the methods and techniques and have become the prominent measurement gauge in various fields such as machine learning and many others.

ACKNOWLEDGMENT

The authors would like to thank the Ministry of Higher Education Malaysia (MoHE) and Universiti Tenaga Nasional for funding this study under the Fundamental Research Grant Scheme (FRGS) of Grant No; FRGS/1/2017/ICT03/UNITEN/03/1

REFERENCES

[1] L. Zhang and L. Zhang Big, “Big Data Analytics for Fault Detection and its Application in Maintenance Operation and Maintenance Engineering.”

[2] D. (Daphne) Yao, X. Shu, L. Cheng, S. J. Stolfo, E. Bertino, and R. Sandhu, “Anomaly Detection as a Service: Challenges, Advances, and Opportunities,” *Synth. Lect. Inf. Secur. Privacy, Trust*, vol. 9, no. 3, pp. 1–173, Oct. 2017.

[3] G. J. Gelatti, A. C. P. de L. F. de Carvalho, and P. P. Rodrigues, “Anomaly Detection Through Temporal Abstractions on Intensive Care Data: Position Paper,” in *2017 IEEE 30th International Symposium on Computer-Based Medical Systems (CBMS)*, 2017, pp. 354–355.

[4] M. Ahmed, A. Naser Mahmood, and J. Hu, “A survey of network anomaly detection techniques,” *Journal of Network and Computer Applications*, vol. 60. Academic Press, pp. 19–31, 01-Jan-2016.

[5] X. Dai and M. Bikdash, “Distance-based outliers method for detecting disease outbreaks using social media,” in *SoutheastCon 2016*, 2016, pp. 1–8.

[6] S. Haque, M. Rahman, S. Aziz, S. A. Haque, M. Rahman, and S. M. Aziz, “Sensor Anomaly Detection in Wireless Sensor Networks for Healthcare,” *Sensors*, vol. 15, no. 4, pp. 8764–8786, Apr. 2015.

[7] C. Jiang, J. Song, G. Liu, L. Zheng, and W. Luan, “Credit Card Fraud Detection: A Novel Approach Using Aggregation Strategy and Feedback Mechanism,” *IEEE Internet Things J.*, pp. 1–1, 2018.

[8] N. Schwenzfeier and V. Gruhn, “Towards a practical process model for anomaly detection systems,” in *Proceedings of the 1st International*

Workshop on Software Engineering for Cognitive Services - SE4COG '18, 2018, pp. 41–44.

[9] X. Shu, D. (Daphne) Yao, N. Ramakrishnan, and T. Jaeger, "Long-Span Program Behavior Modeling and Attack Detection," *ACM Trans. Priv. Secur.*, vol. 20, no. 4, pp. 1–28, Sep. 2017.

[10] F. Sönmez, M. Zontul, O. Kaynar, and H. Tutar, "Anomaly Detection Using Data Mining Methods in IT Systems: A Decision Support Application," *Sak. Univ. J. Sci.*, pp. 1–1, Aug. 2018.

[11] S. Jose, D. Malathi, B. Reddy, and D. Jayaseeli, "A Survey on Anomaly Based Host Intrusion Detection System," *J. Phys. Conf. Ser.*, vol. 1000, no. 1, p. 012049, Apr. 2018.

[12] M. Solanki and V. Dhamdhere, "Intrusion Detection Technique using Data Mining Approach: Survey," *Int. J. Innov. Res. Comput. Commun. Eng. (An ISO*, vol. 3297, no. 11, 2014.

[13] V. Garcia-Font, C. Garrigues, and H. Rifà-Pous, "A Comparative Study of Anomaly Detection Techniques for Smart City Wireless Sensor Networks," *Sensors*, vol. 16, no. 6, p. 868, Jun. 2016.

[14] K. Nian, H. Zhang, A. Tayal, T. Coleman, and Y. Li, "Auto insurance fraud detection using unsupervised spectral ranking for anomaly," *J. Financ. Data Sci.*, vol. 2, no. 1, pp. 58–75, Mar. 2016.

[15] D. Huang, D. Mu, L. Yang, and X. Cai, "CoDetect: Financial Fraud Detection With Anomaly Feature Detection," *IEEE Access*, vol. 6, pp. 19161–19174, 2018.

[16] Z. Zojaji, R. Ebrahimi Atani, and A. Hassan Monadjemi, "A Survey of Credit Card Fraud Detection Techniques: Data and Technique Oriented Perspective."

[17] M. Hauskrecht, I. Batal, M. Valko, S. Visweswaran, G. F. Cooper, and G. Clermont, "Outlier detection for patient monitoring and alerting.," *J. Biomed. Inform.*, vol. 46, no. 1, pp. 47–55, Feb. 2013.

[18] N. Jafarpour Khameneh, "Machine Learning for Disease Outbreak Detection using Probabilistic Models," 2014.

[19] Anders Host-Madsen, "Cardiac monitoring and diagnostic systems, methods, and devices," Jun. 2015.

[20] M. A. Vasarhelyi and H. Issa, "Application of Anomaly Detection Techniques to Identify Fraudulent Refunds."

[21] R. Kaur and S. Singh, "A survey of data mining and social network analysis based anomaly detection techniques," *Egypt. Informatics J.*, vol. 17, no. 2, pp. 199–216, Jul. 2016.

[22] N. Görnitz NICOGOERNITZ, K. Rieck KONRADRIECK, and U. Brefeld, "Toward Supervised Anomaly Detection Marius Kloft," 2013.

[23] C. C. Aggarwal, "Supervised Outlier Detection," in *Outlier Analysis*, New York, NY: Springer New York, 2013, pp. 169–198.

[24] R. Hassanzadeh and R. Nayak, "A semi-supervised graph-based algorithm for detecting outliers in online-social-networks," in *Proceedings of the 28th Annual ACM Symposium on Applied Computing - SAC '13*, 2013, p. 577.

[25] D. Kwon *et al.*, "A survey of deep learning-based network anomaly detection."

[26] Z. Zhao, C. K. Mohan, and K. G. Mehrotra, "Adaptive Sampling and Learning for Unsupervised Outlier Detection," pp. 460–465.

[27] Y. Chae, "Representing Statistical Network-Based Anomaly Detection by Using Trust."

[28] M. A. Rassam, A. Zainal, and M. A. Maarof, "Advancements of data anomaly detection research in Wireless Sensor Networks: A survey and open issues," *Sensors (Switzerland)*, vol. 13, no. 8, pp. 10087–10122, 2013.

[29] W. H. Finch, J. E. Bolin, K. Kelley, J. E. Bolin, and K. Kelley, *Multilevel Modeling Using R*. CRC Press, 2016.

[30] G. Thatte, U. Mitra, and J. Heidemann, "Parametric methods for anomaly detection in aggregate traffic," *IEEE/ACM Trans. Netw.*, vol. 19, no. 2, pp. 512–525, Apr. 2011.

[31] X. Liu and P. S. Nielsen, "Regression-based Online Anomaly Detection for Smart Grid Data," Jun. 2016.

[32] M. Farshchi, J. G. Schneider, I. Weber, and J. Grundy, "Metric selection and anomaly detection for cloud operations using log and metric correlation analysis," *J. Syst. Softw.*, vol. 137, pp. 531–549, Mar. 2018.

[33] A. Zimek and E. Schubert, "Outlier Detection," in *Encyclopedia of Database Systems*, New York, NY: Springer New York, 2017, pp. 1–5.

[34] J. Wu, W. Zeng, and F. Yan, "Hierarchical Temporal Memory method for time-series-based anomaly detection," *Neurocomputing*, vol. 273, pp. 535–546, Jan. 2018.

[35] S. Zou, Y. Liang, H. V. Poor, and X. Shi, "Unsupervised nonparametric anomaly detection: A kernel method," in *2014 52nd Annual Allerton Conference on Communication, Control, and Computing, Allerton 2014*, 2014, pp. 836–841.

[36] M. Bertini, A. Del Bimbo, and L. Seidenari, "Multi-scale and real-time non-parametric approach for anomaly detection and localization," *Comput. Vis. Image Underst.*, vol. 116, no. 3, pp. 320–329, Mar. 2012.

[37] Y. Yilmaz, "Online Nonparametric Anomaly Detection based on Geometric Entropy Minimization," 2017.

[38] L. Yu and Z. Lan, "A Scalable, Non-Parametric Method for Detecting Performance Anomaly in Large Scale Computing," *IEEE Trans. Parallel Distrib. Syst.*, vol. 27, no. 7, pp. 1902–1914, Jul. 2016.

[39] T. M. (Tom M. Mitchell, *Machine Learning*. McGraw-Hill, 1997.

[40] D. B. Araya, K. Grolinger, H. F. ElYamany, M. A. M. Capretz, and G. Bitsuamlak, "An ensemble learning framework for anomaly detection in building energy consumption," *Energy Build.*, vol. 144, pp. 191–206, Jun. 2017.

[41] M. H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita, "Network Anomaly Detection: Methods, Systems and Tools," *IEEE Commun. Surv. Tutorials*, vol. 16, no. 1, pp. 303–336, 2014.

[42] A. H. Moghaddam, M. H. Moghaddam, and M. Esfandyari, "Stock market index prediction using artificial neural network," *J. Econ. Financ. Adm. Sci.*, vol. 21, no. 41, pp. 89–93, Dec. 2016.

[43] D. Heckerman, "Bayesian Networks for Data Mining," *Data Min. Knowl. Discov.*, vol. 1, pp. 79–119, 1997.

[44] J. Yang, J. Deng, S. Li, and Y. Hao, "Improved traffic detection with support vector machine based on restricted Boltzmann machine," *Soft Comput.*, vol. 21, no. 11, pp. 3101–3112, Jun. 2017.

[45] M. Syafiq, M. Pozi, · Md, N. Sulaiman, N. Mustapha, and T. Perumal, "Improving Anomalous Rare Attack Detection Rate for Intrusion Detection System Using Support Vector Machine and Genetic Programming," *Neural Process Lett*, vol. 44, no. 2, pp. 279–290, Oct. 2016.

[46] A. P. Muniyandi, R. Rajeswari, and R. Rajaram, "Network anomaly detection by cascading k-Means clustering and C4.5 decision tree algorithm," in *Procedia Engineering*, 2012, vol. 30, pp. 174–182.

[47] N. M. Zamry, A. Zainal, and M. A. Rassam, "Unsupervised Anomaly Detection for Unlabelled Wireless Sensor Networks Data," 2018.

[48] M. Sabokrou, M. Fayyaz, M. Fathy, Z. Moayedd, and R. klette, "Deep-Anomaly: Fully Convolutional Neural Network for Fast Anomaly Detection in Crowded Scenes," Sep. 2016.

[49] R. Ul Islam, M. S. Hossain, and K. Andersson, "A novel anomaly detection algorithm for sensor data under uncertainty," *Soft Comput.*, vol. 22, no. 5, pp. 1623–1639, 2018.

[50] R. Hassanzadeh and R. Nayak, "A rule-based hybrid method for anomaly detection in online-social-network graphs," in *Proceedings - International Conference on Tools with Artificial Intelligence, ICTAI*, 2013, pp. 351–357.

[51] T. T. Dang, H. Y. T. Ngan, and W. Liu, "Distance-based k-nearest neighbors outlier detection method in large-scale traffic data," *Int. Conf. Digit. Signal Process. DSP*, vol. 2015–Septe, pp. 507–510, Jul. 2015.

[52] S. Gavalep and S. Kahatep, "Improving Distance Based Unsupervised Outlier Detection using Anti-hubs," *Int. J. Sci. Eng. Appl. Sci.*, no. 2, 2016.

[53] T. R. Bandaragoda, K. M. Ting, D. Albrecht, F. T. Liu, Y. Zhu, and J. R. Wells, "Isolation-based anomaly detection using nearest-neighbor ensembles," *Computational Intelligence*, Wiley/Blackwell (10.1111), 05-Jan-2018.

[54] L. Cao, D. Yang, Q. Wang, Y. Yu, J. Wang, and E. A. Rundensteiner, "Scalable distance-based outlier detection over high-volume data streams," in *Proceedings - International Conference on Data Engineering*, 2014, pp. 76–87.

[55] A. El Attar, R. Khatoun, and M. Lemercier, "Clustering-based anomaly detection for smartphone applications," in *IEEE/IFIP NOMS 2014 - IEEE/IFIP Network Operations and Management Symposium: Management in a Software Defined World*, 2014, pp. 1–4.

[56] A. Christy, M. G. Gandhi, and S. Vaithyasubramanian, "Cluster based outlier detection algorithm for healthcare data," in *Procedia Computer Science*, 2015, vol. 50, pp. 209–215.

[57] S. Chernov, "Detecting cellular network anomalies using the knowledge discovery process," *Univ. JYVÄSKYLÄ*, p. 112, 2015.

[58] D. Choudhary, A. Kejariwal, and F. Orsini, "On the Runtime-Efficacy Trade-off of Anomaly Detection Techniques for Real-Time Streaming Data," 2017.

[59] L. Banjanovic-Mehmedovic, A. Hajdarevic, M. Kantardzic, F. Mehmedovic, and I. Dzananovic, "Neural network-based data-driven modelling of anomaly detection in thermal power plant," *Automatika*, vol. 58, no. 1, pp. 69–79, Jan. 2017.