IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol. 8, Issue.5, May 2020 E-ISSN: 2347-2693

Review of Time Series based Anomaly Detection Techniques

Raghavendran R.[1*], Chaitra B.H.[2]

[1,2]Dept. of Computer Science and Engineering, R.V. College of Engineering, Bengaluru, India

[*]Corresponding Author: raghavendranr.1504@gmail.com, Tel.: + 91 9449907576

DOI: https://doi.org/10.26438/ijcse/v8i5.9499 | Available online at: www.ijcseonline.org

Received: 07/May/2020, Accepted: 12/May/2020, Published: 31/May/2020

Abstract— Time series comprise a big portion of real-world data. Time series analysis is one of the most useful tools for researchers and developers. Anomaly detection is one of the key areas of focus in time series. This paper aims to provide a concise and cogent review of the existing research on the topic. In this paper, some widely accepted views and definitions of time series and anomalies are presented. Then, the various methods of anomaly detection in time series are presented, outlining their underlying mechanism, essential features, advantages and drawbacks. Finally, some common trends and observations are summarized, along with a look on the future directions of the research.

Keywords— Time series; anomaly detection; multivariate time series; deep learning; statistics

I. INTRODUCTION

Data has become abundant due to the increasing complexity of technology. Billions of bytes of data is generated from complex networks, industrial and government system every second. While this data is yet to used effectively in practical scenarios owing to its sheer size and complexity. However, some key pieces of information can be derived from the large quantity of data. Thus, in the age of big data, it is crucial to develop effective ways to abstract the data and obtain the above-mentioned information. The data from these systems is of many types. One of the types of data is chronological in nature and called the time series. Anomaly detection on time series is one of the biggest problems being tackled today. The objective of this paper is to present the reader with a comprehensive of the current state of the time series-based research around anomaly detection.

In domains of STEM it is necessary to use mathematical models to analyse the behaviour of phenomena and systems whose explanation cannot be mathematically postulated [1]. An example of such a model is the Time Series. A TS is formed by sequential measurements over time. More commonly, a TS is made up of points where the time interval between successive points remains constant, i.e. the points are equally spaced over time. Time series have various applications in many fields such as health, military, finance and science, and form a large portion of the data available to us, from network logs to measurements from sensors in a Wireless Sensor Network. Time series techniques are used to analyse the basal structure the data may possess such as autocorrelation or seasonality.

Frequently the given time series contains some abnormal or unexpected events. These events are termed anomalies. Anomaly detection (AD) is the task identifying or recognising these anomalies. Anomalies can hold special significance in the time series. For instance, anomalies in health sensor data can be used to detect health problems like Bradycardia or asthma attacks ahead of time [2]. Time series anomaly detection is also employed in detection of stock market manipulation [3, 4], anomalies in shapes [5], and intrusion detection. There is no fixed definition of an anomaly. As can be seen in aforementioned example, what constitutes an anomaly varies based on the application and context. Thus, many solutions for anomaly detection have been proposed. In this paper, a review and summary of some of the most useful and popular procedures for AD in TS is presented.

The contribution of this paper is to organize and present a clear picture of the state-of-the-art time series anomaly detection methods.

- Time series are increasingly relevant in the current era and this paper aims to shed light on the most recent and promising developments in the field.
- AD is one of the most widespread use cases of TS.

Rest of this paper is organised as follows, Section I contains the introduction for time series-based anomaly detection, Section II contains the related works, Section III contains the methodology, Section IV contains results and Section V presents the conclusion and possible future work.

II. RELATED WORK

The work related to defining time series and anomalies form the base for anomaly detection.

Definition of time series

Time series are a stochastic or random process i.e. they obey the laws of probability. They have a natural temporal ordering and are therefore indexed by time. There are two classes of time series:

- Univariate time series: TS which consist of only one variable observed over a period of time
- Multivariate time series: TS where two or more variables are recorded over a period of time. They consist of multidimensional data recorded over time.

One mathematical definition of Time series is a sequence of chronologically ordered records represented as S = {xi(1),xi(2),…,xi(t),…,xi(n) } where t=1,2,3,…n is known as the time and i=1,2,…,m identifies the variable [6]. Thus, an observation xi(t) is the value of the ith variable at time t. Multivariate time series are complex by nature and cannot be modelled easily. They are usually broken down to a simpler form or analysed in a multi stage method[7].

Definition of anomaly

It is important to define what constitutes an anomaly when performing anomaly detection. Anomalies have been defined in many ways throughout literature. They are known as outliers, exceptions, surprise points or abnormalities. One definition is that anomalies are a small quantity of data that is unusual in some way [8].

A widely accepted definition of anomalies was proposed by Hawkins. According to Hawkins, anomalies are those points or observations that deviate so much from other points that they might be actually caused by an external mechanism [9]. By this definition, anomalies are not random in nature and are indicative of some underlying mechanism which can be detected or modelled. Hence, it is suitable for defining problems in application specific time series anomaly detection research.

Anomaly detection in TS can be classified as follows :-

- **Based on statistics**: This is the most studied and oldest method. It involves using the past observations to create a statistical model or distribution. New values are compared to the value in the distribution. If their difference exceeds a value or lies outside a given interval, the the new value is detected as an anomaly. Statistical method can further be classified as:
  1. **Distribution based**: assuming or fitting time series to a known distribution such as a Gaussian distribution or Poission distribution. Anomalies are detected when points are not consistent with the distribution. This method is used for single dimensional data.
  2. **Depth based**: in this method, data points are having n dimensions and a fixed depth. Any point which is at a lower depth than expected is considered an anomaly. Since it uses contours and depths, it is computationally expensive and inefficient when data points have more than three dimensions [10]. JiNao's statistical intrusion detection module is an example of the practical application of statistical anomaly detection [11].
- **Based on distance**: Another anomaly detection method relies on the distance between points. If the distance between objects in the sequence and a given data object or data point is large, then it is declared an anomaly. The distance is measured by setting a distance function. One of the earliest distance-based anomaly detection techniques was put forth by Knorr et al [12]. According to Knorr et al [12], for a dataset specified by parameters (p,D), a data object K is an outlier or anomaly if at least p fraction of objects in the dataset lie at a distance greater than or equal to D from K. The above definition has also been extended to various distribution in [12]. Ramaswamy et al proposed another outlier detection method that is based on the distance of a n object from its kth nearest neighbour [13]. Every object is assigned a rank based on its distance to its nearest 'k' neighbour and points which form the top n ranks are affirmed to be anomalies. There are many other distance-based methods based on index, nested loop and element [14]. Distance based algorithms are easier to understand and overcome many of the disadvantages posed by distribution-based methods. However, these methods do have certain caveats. They have higher complexity than other methods. Further, in data having mixed densities, the distance-based method may incorrectly label areas with scattered points as anomalies. The task of setting parameters like p and D is not trivial.

- **Based on density**: Here, the density of a point is compared to that of its surrounding points. A measure called Local Outlier Factor is used to ascertain whether a point is abnormal. If the LOF is high, then the object is an anomaly. The LOF solution was proposed by Breuning et al [15]. Several other methods of anomaly detection based on density have proposed such as Local Sparsity Coefficient by Agyemang et al [16] and Multi-granularity deviation factor by Papadimitriou et al[17]. Density based methods are also known as Proximity based methods.

- **Based on clustering:** Clustering methods are a subset of density-based anomaly detection. The various data objects are clustered and objects that lie far away from the centroid are considered anomalies. Clustering methods are not optimised for anomaly detection. However, even nonspecific clustering methods work well for detecting anomalies and have significant practical applications. DBSCAN, ROCK, K-Means, etc [18] are some clustering algorithms that can be used for anomaly detection in time series. One of the disadvantages of clustering is that the definition of the anomalies is implicit in the process of clustering. So modelling the anomalies themselves is not possible through clustering.

III. METHODOLOGY

LSTMs are a type of RNN capable of processing long sequences of input data. LSTM addresses the problem of vanishing gradients and exploding gradients that ordinary

RNNs encounter with large time series [20]. Thus, they are appropriate for capturing long time series and providing a dependable prediction. Jerome et al used a LSTM network to forecast and detect anomalies in real application metrics[19] . The metrics collected over a period of 9 days was given as the input time series. The proposed LSTM performed better than SARIMA and ETS for the given univariate data set. In Literature [21], Shi et al propose a LSTM network to predict the key performance indicators for web applications. The predicted value is then tested for anomalies by setting an upper and lower limit using the standard deviation and the mean of the dataset. The LSTM model, however, took longer to train and performed relatively worse than the Gradient Based Regression Tree proposed in [21].

Feng et al propose a combination of LSTM networks for time series anomaly detection on data from industrial control system [22]. Their time series model consists of 2 stacked LSTM networks with a softmax activation layer to achieve high degrees of precision. Further, some probabilistic noise is added to prevent the model from being too sensitive to anomalies. The model, however, is not suitable for all types of attack, as document in [22]. LSTMs have also been used in tandem with other machine learning algorithms for anomaly detection. Ergen et al propose a combination of OCSVM and LSTM [23]. A LSTM network is used to obtain fixed length sequences from variable length data sequences. An OC-SVM algorithm is used for anomaly detection. The combined approached performed better than traditional methods.

Ma et al propose an algorithm based on OCSVM for time series 'novelty' detection [24]. The proposed algorithm involves converting time series data into a group of vectors by unrolling the sequence using a time delay embedding process. The phase space vector is used as input to the OC-SVM for anomaly detection. It is to be noted that the phase vectors are not identically and independently distributed and lose some properties like the PAC performance boundary.

RNNs are a type of neural network that allow the past outputs to be used as the input in subsequent operations. RNNs have been used in time series regression, i.e. to predict future values from past values in a time series, as demonstrated by Madhan et al with algorithm using ARIMA, DWT and RNNs to predict computer network traffic [25]. Since RNN's are capable of time series regression, they are naturally adapted for anomaly detection. Nandhuri et al propose a combination of LSTM and GRU for anomaly detection in aircraft data [26]. Their proposed method overcomes many of the limitations faced by MKAD and Cluster AD, namely in handling MTS data without dimensionality reduction.

Another widely used model is the Random Forest. A Random Forest is an ensemble learning method that builds numerous Decision Tress during the training process. The output of a Random Forest is the mode of the decisions made by all the Trees in the RF [27]. RFs have used for anomaly detection in time series extensively. Pelletier et al propose an iterative approach to detecting anomalies, where the outlier detection is performed by Random Forests [28]. Their work was based on real and artificial vegetation datasets. Radivilova et al use Random Forests to detect typical DDoS attacks in network traffic data [29]. The fractal properties of the traffic affected the performance of the anomaly detection system. Anomalies or attacks were detected earlier and with higher probability in traffic with greater difference in fractal properties.

Duque Anton et al use a Random Forest model and a SVM to detect anomalies in Industrial Data, namely the Modbus and OPC UA protocol datasets [30]. The Random Forest model outperforms the SVM, providing higher accuracy, faster convergence and more linear time behaviour.

K Nearest Neighbour algorithm has also been used extensively for anomaly detection. kNN is a non-parametric, supervised learning algorithm that is sensitive to local data. As it is one the most popular algorithms for pattern recognition and outlier detection [31, 32, 33], it has naturally been extended for anomaly detection in time series. Cai et al propose an anomaly detection algorithm based on kNN to detect disturbances in Power Systems [34]. The proposed method named RD-kNN, involves offline modelling and online detection using a strategy for recursively estimating distance metrics and another to select the kth smallest metric. The time series used in [34] is univariate in nature. Liu et al propose an k Nearest Neighbour based anomaly detection framework with improved similarity measures that overcome the limitations of Euclidean distance [35]. The use of Mahalanobis distance [36, 37] and Dynamic Time Warping distance provide an improved measure of similarity in the telemetry data from satellites. Abid et al propose a centralised k Nearest Neighbour algorithm based on Euclidean distance for data from Wireless Sensor Networks [38].

Kao et al propose an anomaly detection framework for UTS based on deep learning and statistics [39]. The TS data is classified into 3 categories, and various algorithms are applied based on the determined type of time series. The Dickey-Fuller test is used check whether a time series is stationary. If the time series is stationary, the means of a large global window and a smaller local window are compared. If their ratio exceeds a preset threshold, an anomaly is declared. For non-stationary time series, periodicity is determined using Fast Fourier Transforms and Pearson correlation coefficient. For periodic TS with period k, anomalies are detected when the ratio of standard deviations of two successive time sliding windows of k exceeds a preset threshold. Nonstationary, non-periodic TS are modelled using a deep neural network consisting of GRU. The deep network proposed in [39] performs better than LSTM networks while being light weight and easier to train.

Kieu et al suggest a deep neural network framework based on Convolutional Neural Networks and LSTM to detect anomalies in multiple time series datasets [40]. The anomaly detection framework consists of autoencoders based on deep learning models. Autoencoder is an unsupervised technique to decrease the dimensionality of input data, thus reducing feature space of the input [41]. The input time series is multidimensional in nature and enriched by computing statistical features. The enriched time series is used as the input to the autoencoders. Since autoencoders won't model the outliers when reconstructing the enriched time series, comparing the original and rebuilt time series will allow outliers to be detected as points in the original time series that differ from their counterparts in the reconstructed time series. Both autoencoders shown to perform almost equally well, with the LSTM based auto encoder performing slightly better than the 2D CNN based autoencoder.

Munir et al propose their DeepAnT algorithm for overcoming the drawbacks of distance and density-based anomaly detection methods in periodic and seasonal time series [42]. The proposed method has a wide-ranging capacity in detecting anomalies, including point and contextual anomalies, and disturbances in time series data. A deep CNN for time series regression on unlabelled time series data. The predictions are then used by the anomaly detector which uses Euclidean distance to find anomalies. The framework has been shown to work in a variety of different contexts. However, it is greatly affected by poor data quality, where anomalies consist of more than 5% of the entire dataset. Further, there is no standard method to tune the hyperparameters of the deep network.

In literature [43], V. Chandola proposed an algorithm for anomaly detection in MTS. The MTS is converted to UTS by subspace monitoring. Anomaly detection on the obtained UTS is perform using a WINCsvm. While this method considers the numerous characteristics of a MTS simultaneously, its performance is limited by sliding window feature vector calculation when the dataset is very large and complex.

Naoya T proposed an outlier detection algorithm based on semi-supervised learning for multivariate time series [44]. The proposed methodology uses feature extraction and dimensionality reduction to learn the correlation between variables and the temporal relationship within them. While method proposed in the study is novel, the complexity of computation increases many-fold with larger MTS datasets. This drawback was also seen in many other methodologies for MTS data in the available literature.

The above methodologies cover the bulk of the existing time series research. The above techniques have also been used in other anomaly detection systems, like fraud detection in insurance [45] and ranking systems [46]. Other similar applications include crop protection [47] and network control [48].

IV. RESULTS AND DISCUSSION

Anomaly detection on multivariate time series is not well developed in literature. This is due to the following reasons:

- Lack of plentiful data: Since the amount of useful multivariate data is very limited, the research on the matter is also bound by data constraints. Further, the nature of MTS data is unintuitive without mathematical transforms. Thus, defining an anomaly for a multivariate dataset is also a challenge
- Complexity: The variables in a multivariate dataset are usually correlated to a large extent. These complex relationships introduce nonlinearity in the dataset, which makes it infeasible to analyse by traditional statistics and simple models like ARMA. The existing research on MTS data mostly opt for deep learning approaches. While these deep networks are capable of processing MTS data, they also suffer from performance degradation on large datasets. Further, it is often difficult to distinguish actual data from noise interference due to the high dimensionality of the data.
- Curse of dimensionality: MTS data has a large number of dimensions, which takes a heavy toll on the performance of existing algorithm. Many of concepts used in the processing of UTS data become useless when handling MTS data. For example, the distance to the nearest neighbour of a given object may be equal to the distance to the farthest neighbour.

Thus, there are not many real time applications involving MTS.

The most popular approach to handling multivariate time series is to perform feature space reduction and convert it to a simpler UTS. However, this approach has the risk of losing some useful and important correlation within the variables. Some of the recent research in MTS are aiming to reduce the dimensions while retaining the important correlations between the variables.

V. CONCLUSION AND FUTURE SCOPE

To summarise, there is an abundance of data and a large portion of it is comprised of time series. The time series data contains some unusual data called anomalies. The definition of these anomalies varies based on the application. Thus, these definition are made when designing the algorithm or framework to be used. Also, since these definitions are specific to field and application, anomalies can also be considered special patterns or sequences that indicate some other underlying process.

The research on UTS time series is abundant. Many methods have been proposed involving clustering, distances, distributions, probability and statistics. The performance of these methods are also high and well documented. On the contrary, the research on MTS data is very limited due to its high dimensionality and complex nature. It is very different from UTS and many of the most popular methods are not applicable for MTS data. MTS data has the added property of having temporal ordering, which makes it significantly different from other types of multivariate or multidimensional data.

In this survey, many popular algorithms and frameworks for anomaly detection on time series data have been reviewed. The research on MTS data is yet to be fully realised. However, many new promising methodologies are being currently investigated.

REFERENCES

[1] Gómez, J.A., Jaraiz, M.D., Vega, M.A. and Sánchez, J.M. (2008). Optimization of Time Series Using Parallel, Adaptive, and Neural Techniques. In Optimization Techniques for Solving Complex Problems (eds A.Y. Zomaya, E. Alba, C. Blum, P. Isasi, C. León and J.A. Gómez). doi:10.1002/9780470411353.ch8

[2] A. Hosseini and M. Sarrafzadeh, "Unsupervised Prediction of Negative Health Events Ahead of Time," 2019 IEEE EMBS International Conference on Biomedical & Health Informatics (BHI), Chicago, IL, USA, 2019, pp. 1-4.

[3] K. Golmohammadi and O. R. Zaiane, "Time series contextual anomaly detection for detecting market manipulation in stock market," 2015 IEEE International Conference on Data Science and Advanced Analytics (DSAA), Paris, 2015, pp. 1-10.

[4] Z. Ferdousi and A. Maeda, "Unsupervised Outlier Detection in Time Series Data," 22nd International Conference on Data Engineering Workshops (ICDEW'06), Atlanta, GA, USA, 2006, pp. x121-x121.

[5] L. Wei, E. Keogh and X. Xi, "SAXually Explicit Images: Finding Unusual Shapes," Sixth International Conference on Data Mining (ICDM'06), Hong Kong, 2006, pp. 711-720.

[6] H. Wu, "A survey of research on anomaly detection for time series," 2016 13th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP), Chengdu, 2016, pp. 426-431.

[7] V. l. Gorokhov and D. V. Kholodnyak, "Nonparametric statistics in multivariate time series for cognitive anomaly detection," 2016 XIX IEEE International Conference on Soft Computing and Measurements (SCM), St. Petersburg, 2016, pp. 435-436.

[8] Whitehead. B, Hoyt. W. A, "Function approximation approach to anomaly detection in propulsion system test data", Journal of Propulsion and Power, vol.11, no.5, pp. 1074-1076, May, 2015.

[9] Hawkins D.M. (1980) Introduction. In: Identification of Outliers. Monographs on Applied Probability and Statistics. Springer, Dordrecht

[10] Ruts. I, Rousseeuw.P, "Computing depth contours of bivariate point clouds", Computational statistics and data analysis, Vol.23, No.1, pp.153-168, Jan, 1996

[11] Diheng Qu et al., "Statistical anomaly detection for link-state routing protocols," Proceedings Sixth International Conference on Network Protocols (Cat. No.98TB100256), Austin, TX, USA, 1998, pp. 62-70.

[12] Knorr. E. M, Ng. R. T, "A unified notion of outliers: properties and computation", Proceeding of the 3rd international conference on knowledge discovery and data mining, Newport Beach, pp.219-222, Aug, 1997.

[13] Ramaswamy. S, Rastogi. R, Shim. K, "Efficient algorithms for mining outliers from large data sets", Proceeding of the 2000 ACM SIGMOD international conference on management of data, New York, pp. 427-438, Jul, 2000.

[14] Dazhuo Zhou, "Clustering, similarity search and outlier detection in multivariate time series", Tianjing University, Tianjing, 2008.

[15] Breunig, Markus M., et al. "LOF: identifying density-based local outliers." Proceedings of the 2000 ACM SIGMOD international conference on Management of data. 2000.

[16] Agyemang. M, Ezeife. C. I, "Large scale Mine. Algorithm for mining local outliers", Proceeding of the 15th information resource management association international conference, New Orleans, pp.5-8, Apr, 2004.

[17] Papadimitriou. S, Kitagawa. H, Gibbons. P. B, "LOCI fast outlier detection using the local correlation ingral", Technical report, pp.2-9, 2002.

[18] Hardin. J, Rocke. D. M, "Outlier detection in the multiple cluster Setting using the minimum covariance determinant estimator", Computational Statistics and Data Analysis, Vol.44, No.4, pp.625-638, Apr, 2004.

[19] A. Jerome, T. Ishii and H. Chen, "Forecasting and Anomaly Detection on Application Metrics using LSTM," 2018 IEEE International Conference on Big Data (Big Data), Seattle, WA, USA, 2018, pp. 2221-2227.

[20] S. Hochreiter and J. Schmidhuber. "Long Short-Term Memory," Neural Computation 9, 8 November 1997, 1735-1780.

[21] J. Shi, G. He and X. Liu, "Anomaly Detection for Key Performance Indicators Through Machine Learning," 2018 International Conference on Network Infrastructure and Digital Content (IC-NIDC), Guiyang, 2018, pp. 1-5.

[22] C. Feng, T. Li and D. Chana, "Multi-level Anomaly Detection in Industrial Control Systems via Package Signatures and LSTM Networks," 2017 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), Denver, CO, 2017, pp. 261-272.

[23] T. Ergen and M. Kerpiççi, "A novel anomaly detection approach based on neural networks," 2018 26th Signal Processing and Communications Applications Conference (SIU), Izmir, 2018, pp. 1-4.

[24] J. Ma and S. Perkins, "Time-series novelty detection using one-class support vector machines," Proceedings of the International Joint Conference on Neural Networks, 2003., Portland, OR, 2003, pp. 1741-1745 vol.3.

[25] R. Madan and P. S. Mangipudi, "Predicting Computer Network Traffic: A Time Series Forecasting Approach Using DWT, ARIMA and RNN," 2018 Eleventh International Conference on Contemporary Computing (IC3), Noida, 2018, pp. 1-5.

[26] A. Nanduri and L. Sherry, "Anomaly detection in aircraft data using Recurrent Neural Networks (RNN)," 2016 Integrated Communications Navigation and Surveillance (ICNS), Herndon, VA, 2016, pp. 5C2-1-5C2-8.

[27] Asoke K. Nandi; Hosameldin Ahmed, "Decision Trees and Random Forests," in Condition Monitoring with Vibration Signals: Compressive Sampling and Learning Algorithms for Rotating Machines , IEEE, 2019, pp.199-224

[28] C. Pelletier, S. Valero, J. Inglada, G. Dedieu and N. Champion, "New iterative learning strategy to improve classification systems by using outlier detection techniques," 2017 IEEE International Geoscience and Remote Sensing Symposium (IGARSS), Fort Worth, TX, 2017, pp. 3676-3679.

[29] T. Radivilova, L. Kirichenko, D. Ageiev and V. Bulakh, "Classification Methods of Machine Learning to Detect DDoS Attacks," 2019 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), Metz, France, 2019, pp. 207-210

[30] S. D. D. Anton, S. Sinha and H. Dieter Schotten, "Anomaly-based Intrusion Detection in Industrial Data with SVM and Random Forests," 2019 International Conference on Software, Telecommunications and Computer Networks (SoftCOM), Split, Croatia, 2019, pp. 1-6.

[31] P. Yang and B. Huang, "KNN Based Outlier Detection Algorithm in Large Dataset," 2008 International Workshop on Education Technology and Training & 2008 International Workshop on Geoscience and Remote Sensing, Shanghai, 2008, pp. 611-613.

[32] T. T. Dang, H. Y. T. Ngan and W. Liu, "Distance-based k-nearest neighbors outlier detection method in large-scale traffic data," 2015 IEEE International Conference on Digital Signal Processing (DSP), Singapore, 2015, pp. 507-510.

[33] Asniar and K. Surendro, "Using data science for detecting outliers with k Nearest Neighbors graph," 2014 International

Conference on ICT For Smart Society (ICISS), Bandung, 2014, pp. 300-304.

[34] L. Cai, N. F. Thornhill, S. Kuenzel and B. C. Pal, "Real-Time Detection of Power System Disturbances Based on k -Nearest Neighbor Analysis," in IEEE Access, vol. 5, pp. 5631-5639, 2017.

[35] D. Liu, J. Pang, B. Xu, Z. Liu, J. Zhou and G. Zhang, "Satellite Telemetry Data Anomaly Detection with Hybrid Similarity Measures," 2017 International Conference on Sensing, Diagnostics, Prognostics, and Control (SDPC), Shanghai, 2017, pp. 591-596.

[36] PC Mahalanobis, "On the generalised distance in statistics", Proceedings of the National Institute of Sciences of India, 2, 49-55, 1936

[37] R. De Maesschalck, D. Jouan-Rimbaud, D.L. Massart, "The Mahalanobis distance", Chemometrics and Intelligent Laboratory Systems, Volume 50, Issue 1, 2000, Pages 1-18, ISSN 0169-7439

[38] A. Abid, A. Kachouri, A. Ben Fradj Guiloufi, A. Mahfoudhi, N. Nasri and M. Abid, "Centralized KNN anomaly detector for WSN," 2015 IEEE 12th International Multi-Conference on Systems, Signals & Devices (SSD15), Mahdia, 2015, pp. 1-4.

[39] J. Kao and J. Jiang, "Anomaly Detection for Univariate Time Series with Statistics and Deep Learning," 2019 IEEE Eurasia Conference on IOT, Communication and Engineering (ECICE), Yunlin, Taiwan, 2019, pp. 404-407.

[40] T. Kieu, B. Yang and C. S. Jensen, "Outlier Detection for Multidimensional Time Series Using Deep Neural Networks," 2018 19th IEEE International Conference on Mobile Data Management (MDM), Aalborg, 2018, pp. 125-134.

[41] M.A. Kramer, "Nonlinear principal component analysis using autoassociative neural networks", AIChE Journal, 1991, 37: 233-243. doi:10.1002/aic.690370209

[42] M. Munir, S. A. Siddiqui, A. Dengel and S. Ahmed, "DeepAnT: A Deep Learning Approach for Unsupervised Anomaly Detection in Time Series," in IEEE Access, vol. 7, pp. 1991-2005, 2019.

[43] Chandola. V, "Anomaly detection for symbolic sequences and time series data", The University of Minnesota, Minnesota, 2009.

[44] Naoya. T, Takehisa. Y, "Anomaly detection from multivariate time series with sparse representation", Proceeding of IEEE International Conference on Systems, Man and Cybernetics, San Diego, pp.2651-2656, Oct, 2014.

[45] Namrata Ghuse, Pranali Pawar, Amol Potgantwar, "An Improved Approch For Fraud Detection In Health Insurance Using Data Mining Techniques," *International Journal of Scientific Research in Network Security and Communication*, Vol.5, Issue.3, pp.27-33, 2017

[46] R. Satraboyina, GK. Chakravarthi, "*Discovery of Ranking Fraud Detection System for Mobile Apps*", International Journal of Scientific Research in Computer Science and Engineering, Vol.4, Issue.4, pp.7-10, 2016

[47] Priyanka R.R., Mahesh M., Pallavi S.S., Jayapala G., Pooja M.R., "*Crop Protection by an alert Based System using Deep Learning Concept*", International Journal of Scientific Research in Computer Science and Engineering, Vol.6, Issue.6, pp.47-49, 2018

[48] N. SelvaKumar, M. Rohini, C. Narmada, M. Yogeshprabhu, "Network Traffic Control Using AI," *International Journal of Scientific Research in Network Security and Communication*, Vol.8, Issue.2, pp.13-21, 2020

Authors Profile

Mr. Raghavendran R is an Undergraduate student in his 4rd year studying in the CSE department at R V College of Engineering. He has publications in the IAES International Journal of Artificial Intelligence(IAES IJ-AI) and IEEE funded magazine in SJCE, Mysore. He has carried out 3 UG projects and 1 funded Industry Project while at R V College of Engineering.

Prof. Chaitra B H is an Assistant Professor in the CSE department at R V College of Engineering. She has over 9 years of teaching experience and, has published papers in International Journal of Computer Applications (IJCA) and International Journal of Advanced Research in Computer and Communicatuon Engineering (IJARCCE). Her research interests include Software Engineering and Data Mining