Volume 7, Issue 4, April 2017 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Anomaly Detection in Data Mining: A Review

Jagruti D. Parmar
M.E IT, SVMIT, Bharuch, Gujarat, India

Prof. Jalpa T. Patel
CSE & IT, SVMIT Bharuch, Gujarat, India

Abstract— Anomaly detection is the new research topic to this new generation researcher in present time. Anomaly detection is a domain i.e., the key for the upcoming data mining. The term 'data mining' is referred for methods and algorithms that allow extracting and analyzing data so that find rules and patterns describing the characteristic properties of the information. Techniques of data mining can be applied to any type of data to learn more about hidden structures and connections. In the present world, vast amounts of data are kept and transported from one location to another. The data when transported or kept is informed exposed to attack. Though many techniques or applications are available to secure data, ambiguities exist. As a result to analyze data and to determine different type of attack data mining techniques have occurred to make it less open to attack. Anomaly detection is used the techniques of data mining to detect the surprising or unexpected behaviour hidden within data growing the chances of being intruded or attacked. This paper work focuses on Anomaly Detection in Data mining. The main goal is to detect the anomaly in time series data using machine learning techniques.

Keywords— Anomaly Detection; Data Mining; Time Series Data; Machine Learning Techniques.

I. INTRODUCTION

The improvement of Information Technology has caused huge volume of databases and vast data in several areas. The study of datasets and information technology takes certain increase to an approach to collection and operate this valuable data for supplementary decision making.

Data Mining (DM) is formally defined as the non-trivial process of identifying valid, novel, potentially useful and ultimately understandable patterns in data [1]. From a comparatively unknown technique, adopted by some credit institutions and retailers, data mining has developed into a billion dollar business. Banks used data mining to define the credit worthiness of their applicants, retailers adopt it to choose the optimal layout for their shops and insurance companies rely on DM to recognize possible fake or fraudulent claims [1].

The data mining has grown-up to maturity can also be observed from the fact that most database supplier's offer integrated data mining solutions. These tools enable the procedure of knowledge formation and pay towards the more extent of data mining. In some domains, like crime prevention or bio-informatics, DM is still in its beginning. An unseen assurance describes best of these new applications and the known limitations of data mining are easily elapsed. Besides the proliferation of the possible application fields, it can also be perceived that enhancements to the existing techniques are constantly being ready. These enhancements have effect in many different areas: more accurate and understandable predictions, integration with existing databases, real-time analyses etc. [1].

Anomaly detection is a main problem that has been studied in different research domains and application fields. Various techniques of anomaly detection have been definitely established for assured application areas, while others are more common [2].

Anomaly detection is defines as the problem of finding patterns in data that do not conform to expected behavior. These various patterns are normally denote to as anomalies, outliers, discordant observations, exceptions, aberrations, surprises, peculiarities, or contaminants etc., in different application areas. Of these, anomalies and outliers are two terms used most generally in the perspective of anomaly detection; sometimes interchangeably [2].

Anomaly detection find common usage in a different range of applications like fraud detection for credit cards, insurance, or health care, intrusion detection for cyber-security, fault detection in safety critical systems and military surveillance for enemy activities. The significance of anomaly detection is caused by the statement that anomalies in data decode to important and repeatedly serious, actionable information in a inclusive range of application domains [2].

In this paper, we proposed the anomaly detection in data mining based techniques. Anomaly Detection in Data Mining is new research work that provides the analysis of specific data with using techniques of Data Mining.

Section II and III present a brief summary of data mining and anomaly detection. Section IV presents the literature review for anomaly detection in data mining. And finally the conclusion and future work are there for new researcher.

II. DATA MINING

Data mining is defined as a process which discovers useful patterns from huge amount of database [4]. This process of extracting previously unknown, comprehensible and actionable information from large database it helps to

make crucial business decisions [4]. The Knowledge discovery refers as a process that extracts implicit, potentially useful or previously unknown information from the data. The knowledge discovery process is described in figure 1 [4].

There are several major techniques of data mining have been developed and used in data mining projects recently including association rule, classification, clustering, prediction and sequential patterns etc., are used for knowledge discovery from databases [4].

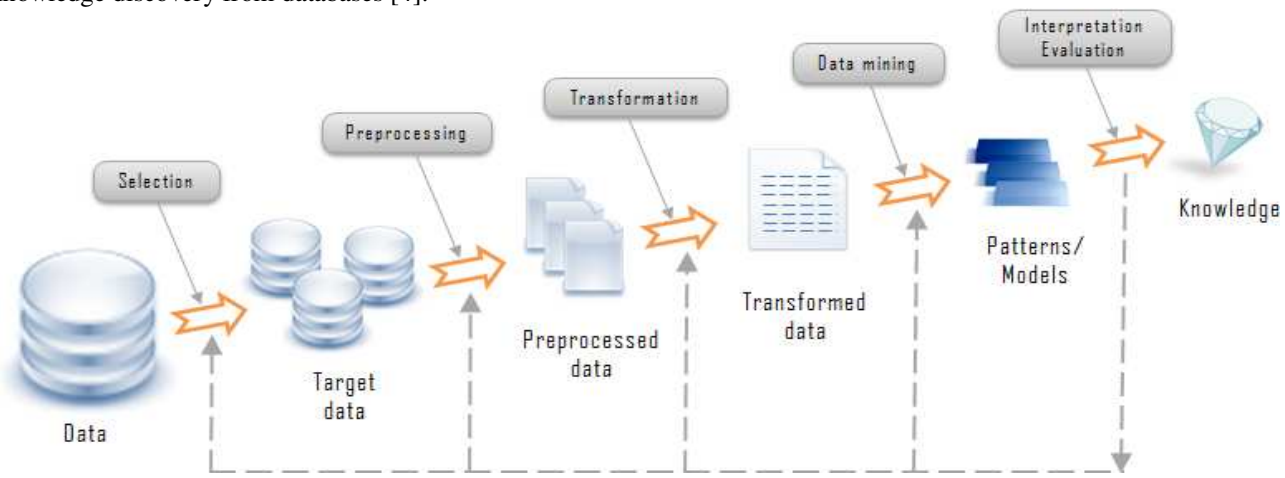

Fig. 1. KDD Process [4]

- **Association:** In this technique, a pattern is exposed based on a relationship of a particular item on other items in the same transaction.
  - Different types of association rules based on
    - → Types of values handled
    - Boolean association rules
    - Quantitative association rules
    - → Levels of abstraction involved
    - Single-level association rules
    - Multilevel association rules
    - → Dimensions of data involved
    - Single-dimensional association rules
    - Multidimensional association rules
  - **Applications**: Market basket data analysis, Cross-marketing, Catalog design, Loss-leader analysis, etc.
- **Classification:** It is a classic data mining technique based on machine learning.
  - It is used to classify each item in a set of data into one of predefined set of classes or groups.
  - It uses of mathematical techniques like decision trees, linear programming, neural network and statistics etc.
  - Classification Techniques :
    - Regression
    - Distance
    - Decision Trees
    - Rules
    - Neural Networks
- **Clustering:** It is the process of establishing objects into groups whose members are similar in some way
  - A cluster is therefore a collection of objects which are 'similar' between them and are 'dissimilar' to the objects belonging to other clusters.
  - Raw data→ clustering algorithms→ cluster of data
- **Prediction:** It discovers relationship between dependent and independent variables.
  - In data mining, autonomous variables are attributes already known and response variables are what we want to predict unfortunately, many real-world problems are not simply prediction.
- **Sequential patterns:** to determine similar patterns in data transaction over a business period. The discover patterns are used for further business analysis to recognize relationships among data.

III. ANOMALY DETECTION

Anomalies are patterns in dataset which do not conform to a well-defined notion of normal behavior [2]. Anomalies cannot always be characterized as attack but it can be a surprising or unexpected behaviour which is previously not known. It may or may not be harmful [5]. Figure 2 illustrates anomalies in a simple two-dimensional data set. The data has two normal regions N1 and N2, since most observations lie in these two regions. Points that are necessarily far away from these regions, for example, the points o1 and o2, and points in region O3 are anomalies [2].

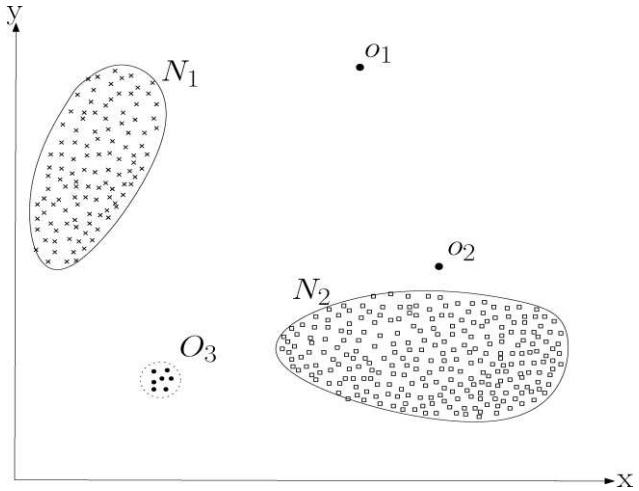

Fig. 2. A simple examples of anomalies in a two dimensional data set [2]

Anomalies might be driven in the dataset for a variety of reasons, like some malicious activity, for example, credit card fraud, cyber-intrusion, terrorist activity or breakdown of a system, but all of the reasons have the common characteristic that they are interesting to the analyst. The interestingness or real life importance of anomalies is a key feature of anomaly detection [2].

Anomaly detection is defined as the process of finding the patterns in a dataset whose behavior is not normal or expected [5]. It is the identification of data points, items, observations or events that do not conform to the expected or known pattern of a given group. These anomalies occur very rarely but may signify a large and significant threat like cyber intrusions or fraud. Anomaly detection is extremely used in behavioral analysis and further methods of analysis such that help in learning about the detection, identification and prediction of the happening of these anomalies [5].

Anomaly detection is primarily a process of data mining and is used to determine the types of anomalies happening in a given data set and to define details about their happenings. It is applicable in domains such as fraud detection, intrusion detection, fault detection, system health monitoring and event detection systems in sensor networks. In the situation of fraud and intrusion detection, the anomalies or interesting patterns are not necessarily the rare items but those unexpected torrents of activities. These types of anomalies do not conform to the definition of anomalies or outliers as rare incidences, so many anomaly detection methods do not work in these instances unless they have been suitably combined or trained. So, in these cases, a cluster analysis algorithm may be more suitable for detecting the micro cluster patterns created by these data points [2]. Figure 3 illustrated the key components associated with an anomaly detection technique.

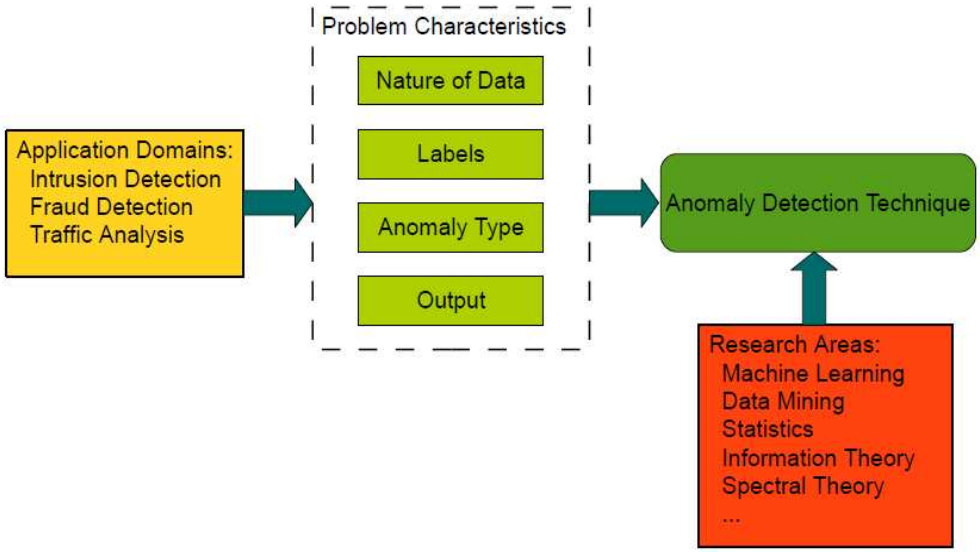

Fig. 3. Key components associated with an anomaly detection technique [2]

A. Type of Anomalies

Anomalies can be classified into these three categories as follows:

(1) Point Anomalies: If an individual data point can be considered as anomalous with respect to the rest of data, then the point is termed a point anomaly [2]. Refer figure 2 as the example of point anomaly.

(2) Contextual Anomalies: If a data point is anomalous in a specific context, but not otherwise, then it is termed a contextual anomaly which also known as conditional anomaly. The notion of a context is induced by the structure in the data set and has to be specified as a part of the problem formulation. Each data point is defined using the following two sets of attributes [1]:

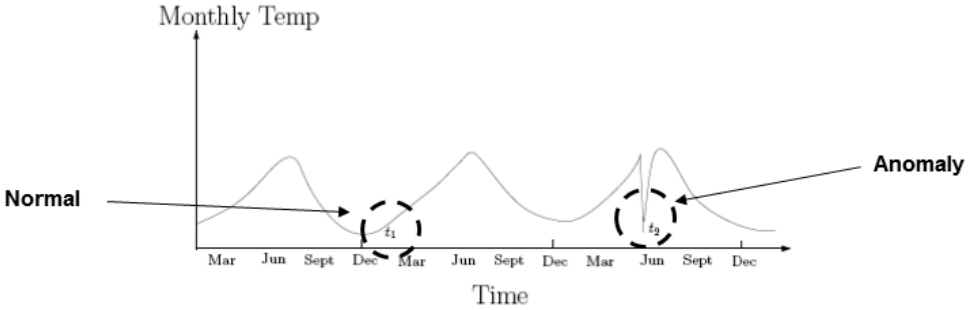

Fig. 4. Example of Contextual anomaly [2]

(a) Contextual attributes: The contextual attributes are used to determine the context or neighborhood for that instance.

(b) Behavioral attributes: The behavioral attributes define the non-contextual characteristics of an instance.

The anomalous behavior is resolute using the values for the behavioral attributes within a specific context. A data instance might be a contextual anomaly in a given context, but an identical data instance, in terms of behavioral attributes could be considered normal in a different context. This characteristic is a key in identify contextual and behavioral attributes for a contextual anomaly detection technique [1].

(3) Collective Anomalies: If a collection of related data instances is anomalous with respect to the entire data set, it is termed a collective anomaly. The individual data instances in a collective anomaly may not be anomalies by themselves, but their existence together as a collection is anomalous [1].

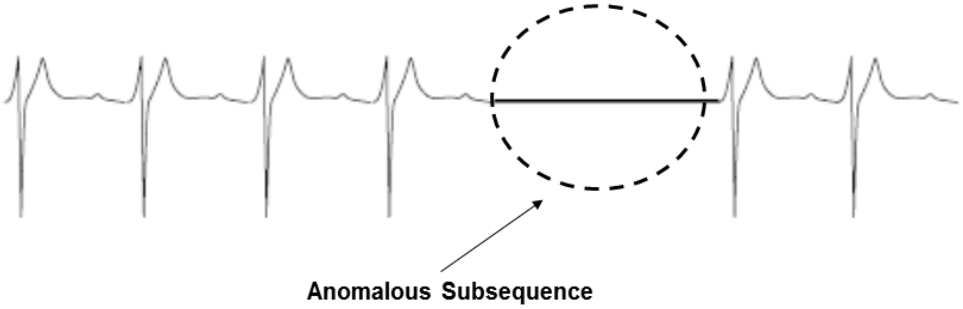

Fig. 5. Example of collective anomaly [2]

B. Data Labels

The labels related with a data point indicate whether that point is normal or anomalous [2]. It should be illustrious that obtaining labeled data that is exact as well as characteristic of all types of behaviors is often too expensive. Labeling is frequently complete by a human expert and hence considerable effort is required to obtain the labeled training data set [2]. Normally, getting a labeled set of anomalous data instances / point that covers all possible type of anomalous behavior is more difficult than receiving labels for normal behavior [2].

Based on the scope which the labels are available, anomaly detection techniques can work on one of the following three modes [2]:

1) Supervised Anomaly Detection: In supervised mode techniques trained with assume the availability of a training data set which has labeled instances for normal as well as anomaly classes.

2) Semi-supervised Anomaly Detection: In semi-supervised mode techniques operate with assume that only for the normal class the training data has labeled instances. Then they do not require labels for the anomaly class, they are more broadly valid than supervised techniques.

3) *Unsupervised Anomaly Detection:* In unsupervised mode techniques operate those do not require training data and hence are most widely applicable. The techniques in this approach type the contained assumption that normal instances are far more frequent than anomalies in the test data. If this assumption is not true then such techniques suffer from high false alarm rate.

C. Output of Anomaly Detection

A significant feature for any anomaly detection technique is the way in which the anomalies are described. Typically, the outputs made by anomaly detection techniques are one of the following two types [2]:

1) Scores: Scoring techniques assign an anomaly score to each point in the test data depending on the degree to which that point is considered an anomaly. Thus the output of such techniques is a ranked list of anomalies. An analyst may select to either analyze the topmost anomalies or use a cutoff threshold to select the anomalies.

2) *Labels:* In this category, techniques assign a label – 'normal' or 'anomalous' to each test instance.

D. General Methodology of Anomaly Detection Technique

While the various anomaly approaches happens, as shown in figure 6 parameter wise train a model prior to detection [5].

1) *Parameterization:* In this stage, the preprocessing data into pre-established arrangements like it is suitable or in agreement with the targeted systems behavior.
2) *Training stage:* In this stage, a model is made on the base of normal or abnormal behavior of the system. There are different ways that can be picked depending on the type of anomaly detection considered. It can be both manual and automatic.
3) *Detection stage:* In this stage, when for the system, the model is available; it is compared with the parameterized or the predefined observed traffic. If the abnormality found beats or is less than when in the case of abnormality models from a predefined threshold then an alarm will be triggered.

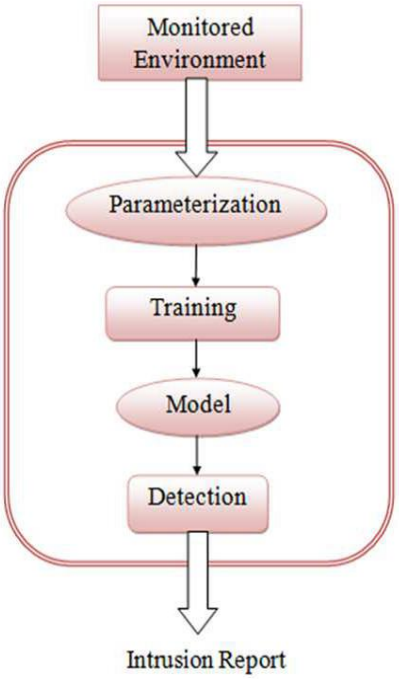

Fig. 6. Methodology of Anomaly Detection [5]

IV. LITERATURE REVIEW

As a part of literature review study research paper is most relevant to anomaly detection in data mining. This survey gives a review on what they have used as method, database for learning and testing, and various different approaches. The review also gives advantages and disadvantages of these methods or future work.

Table I A Review on Anomaly Detection in Data Mining

Sr. No	Publication/ year	Title/ Author	Overview	Advantage	Disadvantage / Future work
1.	IJARCSSE 2012	Data Mining Techniques, Kalyani M Raval [4]	This paper defined data mining and explained the knowledge discovery database (KDD) process. Listed the data mining techniques which is: Association, Classification, Clustering, Prediction and sequential patterns	- Give proper information of data mining. - Listed all the data mining techniques.	- This paper gives overall information of data mining.
2.	ACM 2009	Anomaly Detection: A Survey, Varun Chandola, Arindam Banerjee, And Vipin Kumar [2]	This paper provides structured and comprehensive overview of research on anomaly detection. It includes the definition, challenges, related work, various phases of anomaly detection problem, applications; several types of techniques etc. in short all about of anomaly detection.	- For each category, they find the advantages and disadvantages of the techniques.	- In future, a possible work will be to combine the assumptions completed by several techniques regarding the normal and anomalous behaviour into a statistical or machine learning framework.
3.	ACM 2012	Time-Series Data Mining,	This paper present the purpose of time-series data mining	- Definition as per term used for time	- Try to find more questions and answer

		Philippe Esling And Carlos Agon [5]	which is to try to extract all meaningful knowledge from the shape of data.	series data - Give an overview of the tasks that have captured most of the interest of researchers	raised in data mining for time series data
4.	ACM 2009	Detecting Anomalies in a Time Series Database, Varun Chandola, Deepthi Cheboli, Vipin Kumar [6]	This paper presents a comprehensive evaluation of semi-supervised anomaly detection techniques for time series data. The techniques can be grouped into four categories, i.e., kernel, window, predictive, and segmentation- based techniques.	- This paper represents the several types of datasets for cross-domain experimental evaluation.	- Many combinations of parameters, exhaustive testing could not be done owing to the large parameter space.
5.	Artificial Intelligence Review 2004	A Survey of Outlier Detection Methodologies, Victoria J. Hodge & Jim Austin [7]	This paper presents the methodology of the outlier detection and different approaches (supervised, semi-supervised and unsupervised learning) of the same.	- Describes the models with their outlier detection techniques. - Proper guidance for techniques of outlier detection.	- Study more methods
6.	IEEE 2016	Anomaly Detection In Aircraft Data Using Recurrent Neural Networks (RNN), Anvardh Nanduri and Lance Sherry [8]	This paper describes the application of Recurrent Neural Networks (RNN) for effectively detecting anomalies in flight data.	- RNN based on LSTM and GRU units do not have the limitations of MKAD or Cluster AD as RNNs are by definition capable of handling multivariate sequential input data without any modifications and treat it as time series data. RNNs are also suitable for implementation on the flight deck for real-time anomaly detection.	- to refine the RNNs architecture and training methodology to detect runway change configuration and abnormal pitch anomalies. - Experiments with varying feature combinations may be valuable in assessing the performance of RNN in detecting even the subtlest anomalies in the dataset.
7.	International Journal of Computer Applications 2016	Anomaly based IDS using Backpropagation Neural Network, Vrushali D. Mane and S.N. Pawar [9]	This paper presents the Anomaly Intrusion Detection System that can detect various network attacks. The goal is to identify those attacks with the support of supervised neural network that is. back propagation artificial neural network algorithm and make complete data safe.	- This paper included the data collection from KDD 99 dataset, data pre-processing and normalization, feature reduction, neural network - steps for implementation.	- As the growth of anomaly detection idea through associative analysis, the method can detect not only the problem situations, but also point out the most likely anomaly source.
8.	IEEE 2011	Neural Network Approach to Real-Time Network Intrusion Detection and Recognition, Pavel Kachurka and Vladimir Golovko [10]	This paper introduced recirculation neural network based approach which detects previously undetected attack types in real-time mode and to more correct recognition of these types. The tests detained on both KDD data and real network traffic data prove that this approach can be used in	- Every new detector can be trained using the data samples not recognized by the operating detectors.	- Apply other neural network

			host-based anomaly and misuse detectors.		
9.	IEEE 2009	Host Based Intrusion Detection Using RBF Neural Networks, Usman Ahmed and Asif Masood [11]	This paper presents a novel approach of host based intrusion detection that uses Radial basis Functions Neural Networks (RBFNNs) as profile containers.	- RBFNNs provide better detection rate and very low training time as compared to other soft computing methods.	- Look to implement this approach by adopting a novel activation function other then Gaussian which would hopefully improve the detection capability of the system a lot.
10.	IEEE 2016	Fuzzy Logic Inference for Unsupervised Anomaly Detection, Tetiana Gladkykh, Taras Hnot and Volodymyr Solskyy [12]	This paper introduced the solution for unsupervised anomaly detection i.e., to detect unexpected activity of user or network equipment, based on the analysis of mutual dependencies of the separate slices of network activity.	- Resulting model is an ensemble of fuzzy inference systems, which describe the dependence of the selected parameter from the set of other measured quantities values.	- As the progress of anomaly detection idea through associative analysis, the method can detect not only the problem situations, but also point out the most likely source of the anomaly.
11.	IEEE 2013	Anomaly Detection in Time Series Data using a Fuzzy C-Means Clustering, Hesam Izakian and Witold Pedrycz [13]	This paper presents anomalies in time series which are divided into two categories: amplitude anomalies and shape anomalies. A unified framework sustaining the detection of both types of anomalies is introduced.	- To measure the dissimilarity of each subsequence to different cluster centers, a reconstruction criterion is used.	- -For detecting anomalies in amplitude, the original representation of time series is considered, while for shape anomalies an autocorrelation representation of time series was used.
12.	Proceedings of the Second International Symposium on Networking and Network Security (ISNNS) 2010	An Anomaly Detection Method Based on Fuzzy C-means Clustering Algorithm, Linquan Xie, Ying Wang, Liping Chen, and Guangxue Yue [14]	This paper indicates the fuzzy C-means clustering (FCM) algorithm which applied to detect abnormality which based on network flow.	- It more comprehensively analyzed the data to the clustering, not only helps to reduce the rate of the false alarm and the rate of the failing alarm, at the same time, combine the method with the optimized algorithm of FCM.	- Not efficient so it can further enhance the detection efficiency.
13.	International Journal of Machine Learning and Computing 2014	Effective Clustering of Time-Series Data Using FCM, Saeed Aghabozorgi and Teh Ying Wah [15]	A large part of these successes are due to the novel achieves in dimensionality reduction and distance measurements of time series data. However, addressing the problem of time series clustering through conventional approach has not solved the issue completely, especially when the class label of time series are vague.	- This study indicates the method is more efficient than conventional clustering algorithms computationally, because of less iteration in the learning phase. In terms of being accurate, this method is sufficiently accurate enough in comparison with traditional strategies..	- Needs to be done in order to evaluate the execution algorithm AMCT (Accurate Multilevel Clustering of Time-series) in terms of speed and accuracy of data clusters in different datasets with different dimensions to understand its potentials and limitations.
14.	International	Design Network	This paper introduced an	- The main role of	- In future work

	Journal of Computer Science and Security 2010	Intrusion Detection System using hybrid Fuzzy-Neural Network, Muna Mhammad T. Jawhar and Monica Mehrotra [16]	intrusion detection model based on hybrid fuzzy logic and neural network. The aim is to take advantage of various classification abilities of fuzzy logic and neural network for intrusion detection system.	the present work is to achieve a classification model with high intrusion detection accuracy and mainly with low false negative.	apply another neural network.
15.	IEEE 2004	Adaptive Neuro-Fuzzy Intrusion Detection Systems, Sampada Chavan, Khusbu Shah, Neha Dave and Sanghamitra Mukherjee, Ajith Abraham and Sugata Sanyal [17]	This paper included two machine-learning paradigms, Artificial Neural Networks and Fuzzy Inference System, are used to design an Intrusion Detection System.	- EFuNN performed well compared to neural networks. Experiment results also reveal the importance of input variable reduction.	- The future of IDS lies in data correlation. The IDS of tomorrow will produce results by examining input from several sources.
16.	Elsevier 2010	A new approach to intrusion detection using Artificial Neural Networks and fuzzy clustering, Gang Wang, Jinxing Hao, Jian Ma, and Lihua Huang [18]	This paper presents a new approach, FC-ANN, based on ANN and fuzzy clustering, to solve the problem and help IDS achieve higher detection rate, less false positive rate and stronger stability.	- Propose a new intrusion detection approach, called FC-ANN, based on ANN and fuzzy clustering.	- In future research, how to determine the appropriate number of clustering remains an open problem.
17.	Journal of Computer Science 2013	Hybrid of Fuzzy Clustering Neural Network over Nsl Dataset for Intrusion Detection System, Dahlia Asyiqin Ahmad Zainaddin and Zurina Mohd Hanapi [19]	This paper indicates test the stability of detection precision for low-frequent attacks and weaker detection stability using the current hybrid approach of IDS with NSL dataset instead of using standard KDD Cup 1999 dataset.	- To deal with high poor accuracy and low detection rate has been resolved by the proposed hybrid technique.	- Time consuming
18.	IJERT 2012	Anomaly Based Intrusion Detection System Using Artificial Neural Network and Fuzzy Clustering, Prof. D.P. Gaikwad, Sonali Jagtap, Kunal Thakare and Vaishali Budhawant [20]	This paper work on to add restore point which allows for the rolling back of system files, registry keys, installed programs and the project data base	- The complexity of each sub training set is reduced and consequently the detection performance is increased.	- Apply for this approach only.
19.	European Journal of Advances in Engineering and Technology 2016	A Hybrid Approach of Intrusion Detection using ANN and FCM, Swain Sunita, Badajena J Chandrakanta and Rout Chinmayee [21]	This paper introduced an off-line intrusion detection system is implemented using Multi-Layer Perceptron (MLP) artificial neural network.	- KDD Data set is used for the training and evaluation of the ANN classifier.	- Future work will be use the center values and index values obtained to represent the data pattern and train the system in less iteration.
20.	International Journal of Innovative Research in Computer and Communication Engineering 2016	Hybrid Approach for Classification using Multilevel Fuzzy Min-Max Neural Network, Bhavana Jain and Vaishali Kolhe [22]	This paper proposes the hybrid approach in which pruning strategy has been used to reduce number of hyper boxes and hence accuracy is improved. Various datasets are used for testing purpose.	- The proposed method uses multilevel based FMM technique which gives better accuracy with less number of hyper boxes using pruning strategy.	- This work can be used further for speech classification and text classification.

V. CONCLUSIONS

According to literature review, mostly researcher research on the Anomaly Detection uses data mining and machine leaning techniques or combined both. As par the application anomaly detection it detects. In present time, the anomaly detection in data mining using machine learning technique can be new research area. The main objective is to detect the anomaly in time series data using machine leaning techniques.

In future work, we look forward to implement the approach and perform the comparative analysis with clustering approach for the time series data using artificial neural network, the proposed idea is to be implemented in coming days.

REFERENCES

[1] J. Huysmans, B. Baesens, D. Martens, K. Denys And J. Vanthienen, *New Trends in Data Mining*, Tijdschrift voor Economie en Management, Vol. L, 4, 2005: 1-14.

[2] Varun Chandola, Arindam Banerjee and Vipin Kumar, *Anomaly Detection: A Survey*, ACM Computing Surveys, Vol. 41, No. 3, Article 15, 2009: 1-58.

[3] Animesh Patcha, Jung-Min Park, *An overview of anomaly detection techniques: Existing solutions and latest technological trends*, ScienceDirect 2007.

[4] Kalyani M Raval, *Data Mining Techniques*, International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE) Volume 2, Issue 10, 2012: 439-442.

[5] Philippe Esling and Carlos Agon, *Time-Series Data Mining*, ACM Computing Surveys, Volume 45, No. 1, Article 12 (2012),: 1- 34.

[6] Varun Chandola, Deepthi Cheboli, and Vipin Kumar, *Detecting Anomalies in a Time Series Database*, ACM, Technical Report (2009).

[7] Victoria J. Hodge & Jim Austin, *A Survey of Outlier Detection Methodologies*, Artificial Intelligence Review 22 (2004): 85–126.

[8] Anvardh Nanduri and Lance Sherry, *Anomaly Detection In Aircraft Data Using Recurrent Neural Networks (RNN)*, IEEE Integrated Communications Navigation and Surveillance (ICNS) Conference, 5C2-8(2016):19-21.

[9] Vrushali D. Mane and S.N. Pawar, *Anomaly based IDS using Backpropagation Neural Network*, International Journal of Computer Applications (0975 – 8887) Volume 136 – No.10 (2016):29-34.

[10] Pavel Kachurka and Vladimir Golovko, *Neural Network Approach to Real-Time Network Intrusion Detection and Recognition*, The 6th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications 15-17 (2011): 393-397.

[11] Usman Ahmed and Asif Masood, *Host Based Intrusion Detection Using RBF Neural Networks*, IEEE 2009 International Conference on Emerging Technologies (2009): 48-51.

[12] Tetiana Gladkykh, Taras Hnot and Volodymyr Solskyy, *Fuzzy Logic Inference for Unsupervised Anomaly Detection*, IEEE First International Conference on Data Stream Mining & Processing 23-27 (2016): 42-47.

[13] Hesam Izakian and Witold Pedrycz, *Anomaly Detection in Time Series Data using a Fuzzy C-Means Clustering*, IEEE (2013): 1513-1518.

[14] Linquan Xie, Ying Wang, Liping Chen, and Guangxue Yue, *An Anomaly Detection Method Based on Fuzzy C-means Clustering Algorithm*, Proceedings of the Second International Symposium on Networking and Network Security (ISNNS '10), Academy Publisher, 2-4 (2010): 089-092.

[15] Saeed Aghabozorgi and Teh Ying Wah, *Effective Clustering of Time-Series Data Using FCM*, International Journal of Machine Learning and Computing, Vol. 4, No. 2, (2014): 170-176.

[16] Muna Mhammad T. Jawhar and Monica Mehrotra, *Design Network Intrusion Detection System using hybrid Fuzzy-Neural Network*, International Journal of Computer Science and Security, Volume 4, Issue 3(2010): 285-294.

[17] Sampada Chavan, Khusbu Shah, Neha Dave and Sanghamitra Mukherjee, Ajith Abraham and Sugata Sanyal, *Adaptive Neuro-Fuzzy Intrusion Detection Systems*, IEEE Computer Society Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'04) (2004).

[18] Gang Wang, Jinxing Hao, Jian Ma, and Lihua Huang, *A new approach to intrusion detection using Artificial Neural Networks and fuzzy clustering*, Elsevier Expert Systems with Applications 37 (2010): 6225–6232.

[19] Dahlia Asyiqin Ahmad Zainaddin and Zurina Mohd Hanapi, *Hybrid of Fuzzy Clustering Neural Network over Nsl Dataset for Intrusion Detection System*, Journal of Computer Science, Volume 9, No. 3 (2013): 391-403.

[20] Prof. D.P. Gaikwad, Sonali Jagtap, Kunal Thakare and Vaishali Budhawant, *Anomaly Based Intrusion Detection System Using Artificial Neural Network and Fuzzy Clustering*, International Journal of Engineering Research & Technology (IJERT) Vol. 1 Issue 9 (2012): 1-6.

[21] Swain Sunita, Badajena J Chandrakanta and Rout Chinmayee, *A Hybrid Approach of Intrusion Detection using ANN and FCM*, European Journal of Advances in Engineering and Technology, 3(2), (2016): 6-14.

[22] Bhavana Jain and Vaishali Kolhe, *Hybrid Approach for Classification using Multilevel Fuzzy Min-Max Neural Network*, International Journal of Innovative Research in Computer and Communication Engineering ,Volume 4, Issue 5 (2016): 8636-8640.

