International Journal of Scientific Research in Science, Engineering and Technology

Print ISSN - 2395-1990
Online ISSN : 2394-4099

OPEN ACCESS

Available Online at : www.ijsrset.com
doi : https://doi.org/10.32628/IJSRSET2310662

Traditional Methods and Machine Learning for Anomaly Detection in Self-Organizing Networks

Aakula Lavanya*, Dr. K. Sekar

Department of CSE, Chadalawada Ramanamma Engineering College, Tirupati, Andhra Pradesh, India

ARTICLEINFO

Article History :

Accepted: 10 Dec 2023
Published: 26 Dec 2023

Publication Issue :
Volume 10, Issue 6
November-December-2023
Page Number :
352-360

ABSTRACT

The motivation behind exploring anomaly detection in self-organizing networks lies in the evolving landscape of telecommunications and network management. Conventional methods for identifying network anomalies often struggle to adapt to the dynamic and complex nature of modern self-organizing networks. The problem addressed in this research is the efficacy of anomaly detection methods in self-organizing networks (SONs) within the context of telecommunications and network management. As SONs become increasingly prevalent to meet the demands of modern, highly dynamic wireless communication systems, the need for robust anomaly detection mechanisms is paramount. Conventional anomaly detection approaches in SONs are often based on predefined rules and thresholds, which may struggle to adapt to the intricate and rapidly evolving network behaviors. These methods can result in false alarms, missed anomalies, and inefficient resource allocation. Furthermore, emerging SONs incorporate a multitude of diverse technologies, including 5G, IoT, and edge computing, compounding the complexity of anomaly detection. Contemporary machine learning techniques hold promise in addressing these challenges by enabling the automatic and adaptive detection of anomalies, leveraging the abundance of data generated in SONs. However, the suitability, performance, and scalability of these methods in dynamic and large-scale SON environments remain critical concerns. This research aims to compare and evaluate conventional anomaly detection methods against contemporary machine learning approaches in SONs to assess their accuracy, efficiency, and adaptability. The goal is to provide insights into the most effective anomaly detection strategies, ultimately enhancing network stability, minimizing downtime, and ensuring the secure and efficient operation of modern telecommunications systems.

Keywords : Machine Learning, Anomaly Detection, Self-organizing networks, MIMO, wireless sensor networks.

I. INTRODUCTION

As a next-generation telecommunication technology novel perspective and innovative solutions to the increased demand of humans and autonomous devices. This technology mainly focuses on five areas, including dense-device structures, high carrier frequency bands such as millimetre wave (mmWave), multi-connectivity such as massive MIMO, smart devices, and massive machine-type communications [1]. To fulfill these requirements in such a dynamic digital world, the next-generation cellular networks must be adaptable with predictive capabilities due to the ever changing environment of the nested services interacting with each other. Hence, artificial intelligence (AI) has garnered increased interest as a potential to handle the dynamic environment in analysing and contributing to the execution of the network [2]. There are examples of intelligent applications on massive machine-type communications (mMTC) in 5G or massive MIMO in wireless sensor networks (WSNs), to achieve better service quality through improved IoT connectivity as well as to extend battery life and boost spectral efficiency by utilizing channel aware decision fusion methodology [3], [4]. In previous mobile networks, such as 4G, autonomous mobile networks or self-organizing networks (SONs) with capabilities such as self-planning, self-configuring, self optimizing, and self-healing, have been shown to significantly contribute to reducing network failures and boosting performance without human intervention such as Air Hop's eSON [5]. However, current solutions in the market generally lack smart functionalities, especially for cell outage management (COM) to heal autonomically [6]. If there is no traffic due to a specific network issue, it signals an anomaly where one or more cells may be in outage and it is vital to detect the outage to resume service within the shortest time possible. For instance, Ericsson lost at least $100 million because of a network outage [7], which could have been prevented using AI-powered SONs. In consideration of these issues, the European Telecommunications Standards Institute (ETSI) introduced a zero-touch group to research automation to advance machine learning and AI techniques (deep learning) specifically for anomaly detection applications on mobile networks. This paper has four main contributions to the field as summarized below: We present a comprehensive analysis of a conventional machine learning method for anomaly detection in selforganizing 5G networks (5G-SONs) and compare it with a popular deep learning alternative using different learning representations, including one-class and binary learning. We claim state-of-the-art performance on a publicly available dataset [8], which investigates multiple use case scenarios for anomaly detection in 5G-SONs. We demonstrate an average improvement of 15% over the best recent performance which was achieved by a deep auto-encoder-based setup. We demonstrate for the first time that data augmentation methods can further boost anomaly detection performance in binary mode, even when utilizing conventional algorithmic methods such as support vector machines on a sufficiently large dataset. Finally, we achieve nearly two orders of magnitude improvement in computational speed and an order of magnitude reduction in trainable parameters using conventional machine learning to provide a robust alternative for elf-organizing networks especially when the execution and detection times are critical. The rest of this paper is organized as follows. Section II provides a brief summary of prior work on anomaly detection in current mobile and self-organizing networks. Section III introduces the methods used in this study. Section IV describes the experimental setup in detail and provides the hyper-parameters, dataset characteristics, implementation, evaluation metrics, and necessary details for repeatability. Finally, the results and discussions are presented in Section V, followed by the conclusions in Section VI. The abbreviations used in this paper have been provided in Table 1 for easy reference.

II. RELATED WORKS

Massive MIMO is considered to be one of the key technologies in the emerging 5G systems, but also a concept applicable to other wireless systems. Exploiting the large number of degrees of freedom (DoFs) of massive MIMO is essential for achieving high spectral efficiency, high data rates and extreme spatial multiplexing of densely distributed users. On the one hand, the benefits of applying massive MIMO for broadband communication are well known and there has been a large body of research on designing communication schemes to support high rates. On the other hand, using massive MIMO for Internet-of-Things (IoT) is still a developing topic, as IoT connectivity has

requirements and constraints that are significantly different from the broadband connections [9]. In this paper we investigate the applicability of massive MIMO to IoT connectivity. Specifically, we treat the two generic types of IoT connections envisioned in 5G: massive machine-type communication (mMTC) and ultra-reliable low-latency communication (URLLC). This paper fills this important gap by identifying the opportunities and challenges in exploiting massive MIMO for IoT connectivity [10]. We provide insights into the trade-offs that emerge when massive MIMO is applied to mMTC or URLLC and present a number of suitable communication schemes. The discussion continues to the questions of network slicing of the wireless resources and the use of massive MIMO to simultaneously support IoT connections with very heterogeneous requirements. The main conclusion is that massive MIMO can bring benefits to the scenarios with IoT connectivity, but it requires tight integration of the physical-layer techniques with the protocol design [11].

What will 5G be? What it will not be is an incremental advance on 4G. The previous four generations of cellular technology have each been a major paradigm shift that has broken backward compatibility. Indeed, 5G will need to be a paradigm shift that includes very high carrier frequencies with massive bandwidths, extreme base station and device densities, and unprecedented numbers of antennas. However, unlike the previous four generations, it will also be highly integrative: tying any new 5G air interface and spectrum together with LTE and WiFi to provide universal high-rate coverage and a seamless user experience [12]. To support this, the core network will also have to reach unprecedented levels of flexibility and intelligence, spectrum regulation will need to be rethought and improved, and energy and cost efficiencies will become even more critical considerations. This paper discusses all of these topics, identifying key challenges for future research and preliminary 5G standardization activities, while providing a comprehensive overview of the current literature, and in particular of the papers appearing in this special issue.

We propose an unsupervised learning based anomaly detection framework for identifying cells experiencing performance degradation due to mobility problems, in LTE networks. Handover failure rate is used as a performance metric, whereas the mobility problems considered include too-early and too-late handovers [13]. In order to enable unsupervised learning, the framework leverages existing datasets in commercial LTE networks (e.g. performance management counters, configuration management data, geographical locations, and inventory data etc). To this end, the first step is data pre-processing, followed by feature extraction based on principal component analysis and clustering. For implementation, we use real data from an operational commercial LTE network. Results show that clustering is highly effective in understanding and identifying mobility related anomalous behaviour, and provides actionable insights for automation and self-optimization, paving the way for efficient mobility robustness optimization, which is an important self-optimization use-case for contemporary 4G/5G networks [14].

Self-organizing networks (SON) for cellular systems is emerging as an important technology to reduce the cost of network deployment and maintenances. Mobility robustness optimization (MRO) is one of the main use cases of SON and has been intensively studied in 3GPP working groups. This paper proposes a dynamic self-optimization algorithm for handover (HO) parameters using the Q-Learning method. The proposed algorithm is mobility robustness, which means that the HO performance is robust against the change in UE mobility. In order to realize the mobility robustness, the proposed algorithm adaptively adjusts the HO parameters through Q-learning [15]. This paper examines the performance of the proposed algorithm through the computer simulations and confirms the mobility robustness. The simulation results show that the success rate of Handover (HO) is improved and user experience is enhanced by the Q-MRO algorithm

Anomaly detection is critical given the raft of cyber attacks in the wireless communications these days. It is thus a challenging task to determine network anomaly more accurately. In this paper, we propose an Autoencoder-based network anomaly detection method. Autoencoder is able to capture the non-linear correlations between features so as to increase the detection accuracy. We also apply the Convolutional Autoencoder (CAE) here to perform the dimensionality reduction. As the Convolutional Autoencoder has a smaller number of parameters, it requires less training time compared to the conventional Autoencoder. By evaluating on NSL-KDD dataset, CAE-based network anomaly detection method outperforms other detection methods [16].

III. PROPOSED METHODOLOGY

Proposed several machine learning models model to classify but none have adequately addressed this misdiagnosis problem. That can be used for this purpose are Integrating Machine Learning Anomaly Detection in Self-Organizing Networks Conventional Versus Contemporary. Also, similar studies that have proposed models for evaluation of such tumors mostly do not consider the heterogeneity and the size of the data Therefore, we propose a machine learning-based approach which combines a new technique of preprocessing the data for features transformation, Random Forest Classifier, SVC, K Neighbors Classifier, K Means give the best accuracy techniques to eliminate the bias and the deviation of instability and performing classifier tests based represented in figure 1.

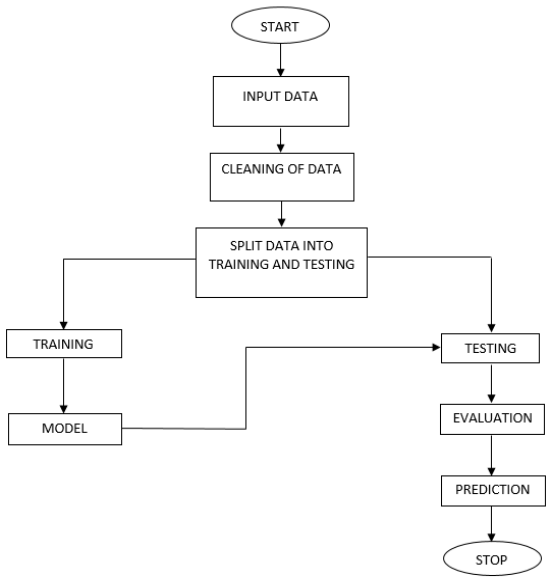

Figure 1: Proposed Methodology of work flow.

Support Vector Machine or SVM is one of the most popular Supervised Learning algorithms, which is used for Classification as well as Regression problems. However, primarily, it is used for Classification problems in Machine Learning. The goal of the SVM algorithm is to create the best line or decision boundary that can segregate n-dimensional space into classes so that we can easily put the new data point in the correct category in the future. This best decision boundary is called a hyper plane. SVM chooses the extreme points/vectors that help in creating the hyper plane. These extreme cases are called as support vectors, and hence algorithm is termed as Support Vector Machine. Consider the below figure 2 in which there are two different categories that are classified using a decision boundary or hyper plane.

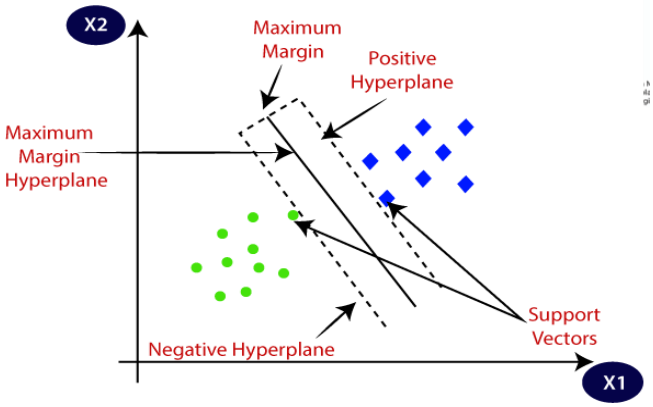

Figure 2: different categories used for decision boundary or hyper plane.

K-NN algorithm stores all the available data and classifies a new data point based on the similarity. This means when new data appears then it can be easily classified into a well suite category by using K- NN algorithm. K-NN algorithm can be used for Regression as well as for Classification but mostly it is used for the Classification problems. K-NN is a non-parametric algorithm, which means it does not make any assumption on underlying data. It is also called a lazy learner algorithm because it does not learn from the training set immediately instead it stores the dataset and at the time of classification, it performs an action on the dataset.

KNN algorithm at the training phase just stores the dataset and when it gets new data, and then it classifies that data into a category that is much similar to the new data. It is also called a lazy learner algorithm because it does not learn from the training set immediately instead it stores the dataset and at the time of classification, it performs an action on the dataset. KNN algorithm at the training phase just stores the dataset and when it gets new data, and then it classifies that data into a category that is much similar to the new data.

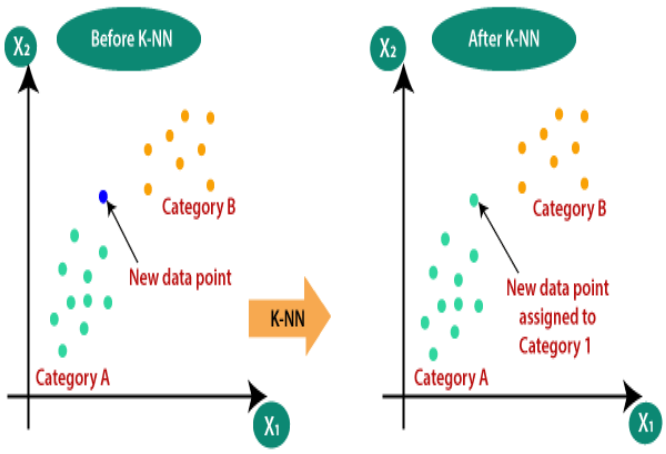

Figure 3: Comparisons between before and after K-NN.

A random forest is a machine learning technique that's used to solve regression and classification problems. It utilizes ensemble learning, which is a technique that combines many classifiers to provide solutions to complex problems.

A random forest algorithm consists of many decision trees. The 'forest' generated by the random forest algorithm is trained through bagging or bootstrap aggregating. Bagging is an ensemble meta-algorithm that improves the accuracy of machine learning algorithms.

The (random forest) algorithm establishes the outcome based on the predictions of the decision trees. It predicts by taking the average or mean of the output from various trees. Increasing the number of trees increases the precision of the outcome.

A random forest eradicates the limitations of a decision tree algorithm. It reduces the over fitting of datasets and increases precision. It generates predictions without requiring many configurations in packages (like Scikit-learn).

Decision trees are the building blocks of a random forest algorithm. A decision tree is a decision support technique that forms a tree-like structure. An overview of decision trees will help us understand how random forest algorithms work.

A decision tree consists of three components: decision nodes, leaf nodes, and a root node. A decision tree algorithm divides a training dataset into branches, which further segregate into other branches. This sequence continues until a leaf node is attained. The leaf node cannot be segregated further.

The nodes in the decision tree represent attributes that are used for predicting the outcome. Decision nodes provide a link to the leaves. The following diagram shows the three types of nodes in a decision tree.

The information theory can provide more information on how decision trees work. Entropy and information gain are the building blocks of decision trees. An overview of these fundamental concepts will improve our understanding of how decision trees are built.

Entropy is a metric for calculating uncertainty. Information gain is a measure of how uncertainty in the target variable is reduced, given a set of independent variables.

The information gain concept involves using independent variables (features) to gain information about a target variable (class). The entropy of the target variable (Y) and the conditional entropy of Y (given X) are used to estimate the information gain. In this case, the conditional entropy is subtracted from the entropy of Y.

Information gain is used in the training of decision trees. It helps in reducing uncertainty in these trees. A high information gain means that a high degree of uncertainty (information entropy) has been removed. Entropy and information gain are important in splitting branches, which is an important activity in the construction of decision trees.

Let's take a simple example of how a decision tree works. Suppose we want to predict if a customer will purchase a mobile phone or not. The features of the phone form the basis of his decision. This analysis can be presented in a decision tree diagram.

The root node and decision nodes of the decision represent the features of the phone mentioned above. The leaf node represents the final output, either buying or not buying. The main features that determine the choice include the price, internal storage, and Random Access Memory (RAM). The decision tree will appear as follows.

The main difference between the decision tree algorithm and the random forest algorithm is that establishing root nodes and segregating nodes is done randomly in the latter. The random forest employs the bagging method to generate the required prediction.

Bagging involves using different samples of data (training data) rather than just one sample. A training dataset comprises observations and features that are used for making predictions. The decision trees produce different outputs, depending on the training data fed to

the random forest algorithm. These outputs will be ranked, and the highest will be selected as the final output. Our first example can still be used to explain how random forests work. Instead of having a single decision tree, the random forest will have many decision trees. Let's assume we have only four decision trees. In this case, the training data comprising the phone's observations and features will be divided into four root nodes.

The root nodes could represent four features that could influence the customer's choice (price, internal storage, camera, and RAM). The random forest will split the nodes by selecting features randomly. The final prediction will be selected based on the outcome of the four trees.

The outcome chosen by most decision trees will be the final choice. If three trees predict buying, and one tree predicts not buying, then the final prediction will be buying. In this case, it's predicted that the customer will buy the phone.

An artificial neural network (ANN) is the piece of a computing system designed to simulate the way the human brain analyses and processes information. It is the foundation of artificial intelligence (AI) and solves problems that would prove impossible or difficult by human or statistical standards. ANNs have self-learning capabilities that enable them to produce better results as more data becomes available.

An ANN has hundreds or thousands of artificial neurons called processing units, which are interconnected by nodes. These processing units are made up of input and output units. The input units receive various forms and structures of information based on an internal weighting system and the neural network attempts to learn about the information presented to produce one output report. Just like humans need rules and guidelines to come up with a result or output, ANNs also use a set of learning rules called back propagation, an abbreviation for backward propagation of error, to perfect their output results.

An ANN initially goes through a training phase where it learns to recognize patterns in data, whether visually, aurally, or textually. During this supervised phase, the network compares its actual output produced with what it was meant to produce—the desired output. The difference between both outcomes is adjusted using back propagation. This means that the network works backward, going from the output unit to the input units to adjust the weight of its connections between the units until the difference between the actual and desired outcome produces the lowest possible error.

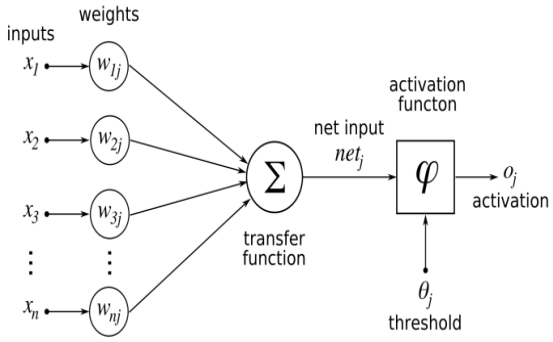

Figure 4 : Architecture of ANN.

K-Means Clustering is an unsupervised learning algorithm that is used to solve the clustering problems in machine learning or data science. In this topic, we will learn what is K-means clustering algorithm, how the algorithm works, along with the Python implementation of k-means clustering.

K-Means Clustering is an Unsupervised Learning algorithm which groups the unlabeled dataset into different clusters. Here K defines the number of pre-defined clusters that need to be created in the process, as if K=2, there will be two clusters, and for K=3, there will be three clusters, and so on.\

It allows us to cluster the data into different groups and a convenient way to discover the categories of groups in the unlabeled dataset on its own without the need for any training.

It is a centroid-based algorithm, where each cluster is associated with a centroid. The main aim of this algorithm is to minimize the sum of distances between the data point and their corresponding clusters.

The algorithm takes the unlabeled dataset as input, divides the dataset into k-number of clusters, and repeats the process until it does not find the best clusters. The value of k should be predetermined in this algorithm.

IV. RESULT ANALYSIS

MODULES:

User:

Register:

Users can register for Anomaly Detection in Self-Organizing Networks Conventional Versus Contemporary Machine Learning application here.

Login:

After registering, the user can access his portal**.**

View Home page:

Here user views the home page of the Students adaptability level application.

View about page:

In the about page, users can learn more about the e-learning platform.

View load data page:

In the load data page, the user will load the dataset for modeling.

Input Model:

The user must provide input values for the certain fields in order to get results.

View Results:

User view's the generated results from the model.

View score:

Here users have ability to view the accuracy score in %

System

Working on dataset:

System checks for data whether it is available or not and load the data in csv files.

Pre-processing:

Data need to be pre-processed according the models it helps to increase the accuracy of the model and better information about the data.

Training the data:

After pre-processing the data will split into two parts as train and test data before training with the given algorithms.

Model Building

To create a model that predicts the personality with better accuracy, this module will help user.

Generated Score:

Here user view the score in %

Generate Results:

We train the machine learning algorithm and predict the Students adaptability level.

RESULTS

Home Page:

In figure 5, here user views the home page of Anomaly Detection in Self-Organizing Networks Conventional Versus Contemporary Machine Learning web application.

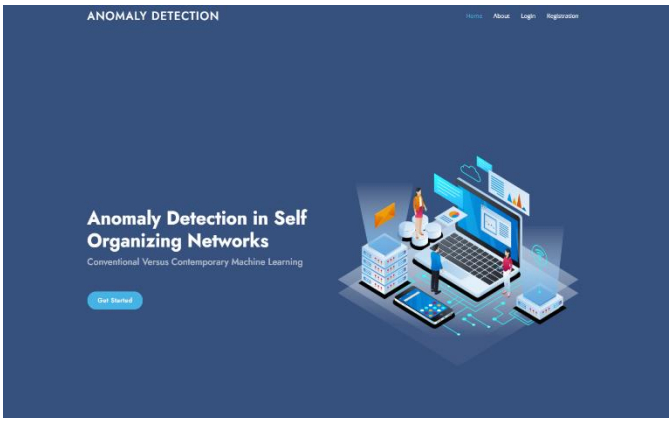

Figure 5: Home page of Anomaly Detection in Self-Organizing Networks

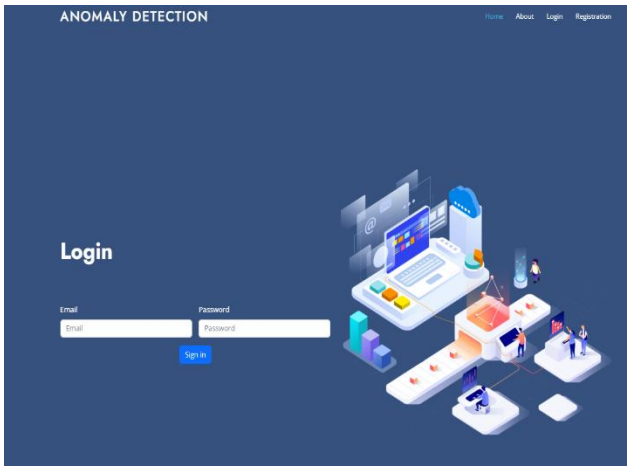

Figure 6: Login Page for anomaly detection.

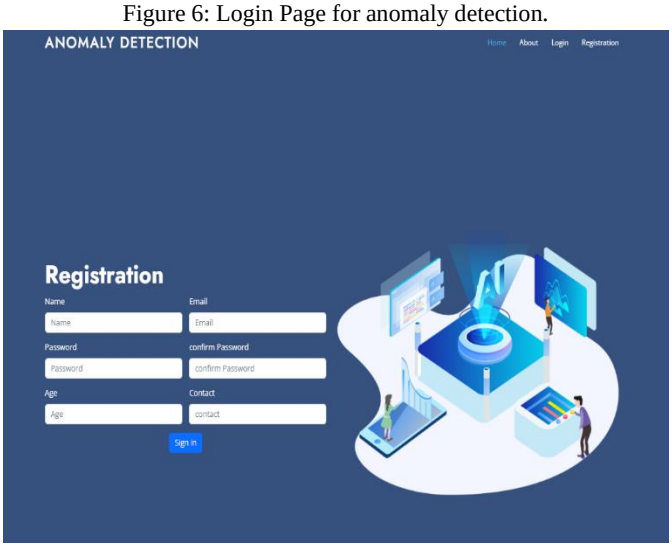

Figure 7: registration Page.

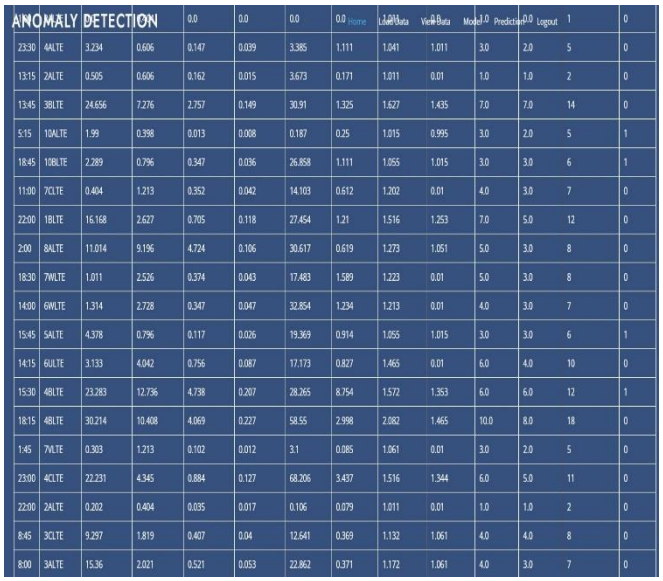

Figure 8 : View page for anomaly detection.

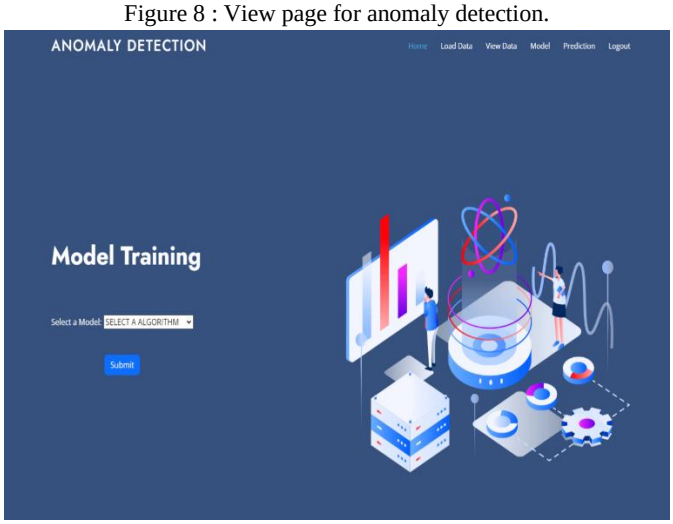

Figure 9 : Model page for selecting algorithm.

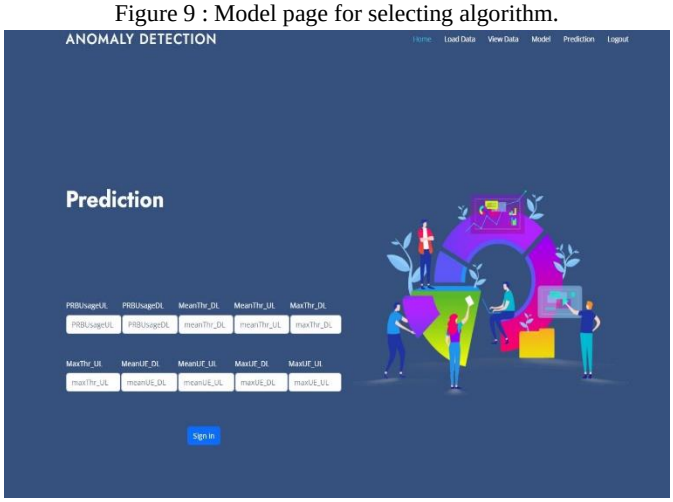

Figure 10: Prediction page for anomaly detection.

V. CONCLUSION

In this paper, we have developed a user friendly application called Integrating Machine Learning Anomaly Detection in Self-Organizing Networks Conventional Versus Contemporary techniques such as support vector machines (SVM), K-nearest neighbor (KNN), Random Forest Classifier, K Means and ANN. We used the best techniques we found and its show the weather it is Anomaly or Not Anomaly.

Future enhancements in anomaly detection for self-organizing networks (SONs) should focus on improving adaptability, scalability, and real-time responsiveness to address the evolving challenges in telecommunications and network management.

Incorporating these future enhancements will lead to more effective, efficient, and adaptable anomaly detection systems in self-organizing networks, ensuring the reliability and security of modern telecommunications and network infrastructures.

VI. REFERENCES

[1]. F. Boccardi, R. W. Heath, A. Lozano, T. L. Marzetta, and P. Popovski, "Five disruptive technology directions for 5G," IEEE Commun. Mag., vol. 52, no. 2, pp. 74–80, Feb. 2014

[2]. J. G. Andrews, S. Buzzi, W. Choi, S. V. Hanly, A. Lozano, A. C. Soong, and J. C. Zhang, "What will 5G be?" IEEE J. Sel. Areas Commun., vol. 32, no. 6, pp. 1065–1082, Jun. 2014.

[3]. A. S. Bana, E. de Carvalho, B. Soret, T. Abrão, J. C. Marinello, E. G. Larsson, and P. Popovski, "Massive MIMO for Internet of Things (IoT) connectivity," Phys. Commun., vol. 37, Dec. 2019, Art. no. 100859.

[4]. D. Ciuonzo, P. S. Rossi, and S. Dey, "Massive MIMO channel-aware decision fusion," IEEE Trans. Signal Process., vol. 63, no. 3, pp. 604–619, Feb. 2015.

[5]. Airhop. Accessed: Jun. 18, 2021. [Online]. Available: http://www. airhopcomm.com

[6]. I. de-la-Bandera, R. Barco, P. Muñoz, and I. Serrano, "Cell outage detection based on handover statistics," IEEE Commun. Lett., vol. 19, no. 7, pp. 1189–1192, Jul. 2015.

[7]. Ericson. Network Outage. Accessed: Jun. 18, 2021. [Online]. Available: http://telecoms.com/494091/

[8]. M. Z. Asghar, M. Abbas, K. Zeeshan, P. Kotilainen, and T. Hämäläinen, ‘‘Assessment of deep learning methodology for self-organizing 5G networks,’’ Appl. Sci., vol. 9, no. 15, p. 2975, Jul. 2019.

[9]. S. Rajendran, W. Meert, V. Lenders, and S. Pollin, ‘‘Unsupervised wireless spectrum anomaly detection with interpretable features,’’ IEEE Trans. Cognit. Commun. Netw., vol. 5, no. 3, pp. 637–647, Sep. 2019.

[10]. J. Burgueño, I. de-la-Bandera, J. Mendoza, D. Palacios, C. Morillas, and R. Barco, ‘‘Online anomaly detection system for mobile networks,’’ Sensors, vol. 20, no. 24, p. 7232, Dec. 2020.

[11]. F. Boccardi, R. W. Heath, A. Lozano, T. L. Marzetta and P. Popovski, "Five disruptive technology directions for 5G", IEEE Commun. Mag., vol. 52, no. 2, pp. 74-80, Feb. 2014.

[12]. J. G. Andrews, S. Buzzi, W. Choi, S. V. Hanly, A. Lozano, A. C. Soong, et al., "What will 5G be?", IEEE J. Sel. Areas Commun., vol. 32, no. 6, pp. 1065-1082, Jun. 2014.

[13]. P. Krishna Kishore, S. Ramamoorthy, V.N. Rajavarman, ARTP: Anomaly based real time prevention of Distributed Denial of Service attacks on the web using machine learning approach, International Journal of Intelligent Networks, Volume 4, 2023, Pages 38-45, ISSN 2666-6030, https://doi.org/10.1016/j.ijin.2022.12.001.

[14]. M. Z. Asghar, M. Abbas, K. Zeeshan, P. Kotilainen and T. Hämäläinen, "Assessment of deep learning methodology for self-organizing 5G networks", Appl. Sci., vol. 9, no. 15, pp. 2975, Jul. 2019.

[15]. P. Krishna Kishore, S. Ramamoorthy, V.N. Rajavarman, "Mitigation of HTTP Flood DDoS Attack in Application Layer Using Machine Learning and Isolation Forest," SSRG International Journal of Electrical and Electronics Engineering, vol. 10, no. 10, pp. 6-19, 2023. Crossref, https://doi.org/10.14445/23488379/IJEEE-V10I10P102

[16]. Krishna Kishore, P., Prathima, K., Eswari, D.S., Goud, K.S. (2023). Bidirectional LSTM-Based Sentiment Analysis of Context-Sensitive Lexicon for Imbalanced Text. In: Bhateja, V., Sunitha, K.V.N., Chen, YW., Zhang, YD. (eds) Intelligent System Design. Lecture Notes in Networks and Systems, vol 494. Springer, Singapore. https://doi.org/10.1007/978-981-19-4863-3_27

Cite this article as :

Aakula Lavanya, Dr. K. Sekar, "Traditional Methods and Machine Learning for Anomaly Detection in Self-Organizing Networks", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 10 Issue 6, pp. 352-360, November-December 2023. Available at doi : https://doi.org/10.32628/IJSRSET2310662
Journal URL : https://ijsrset.com/IJSRSET2310662