Internet of things (IoT) becomes the most popular term in the recent advances in Healthcare devices. The healthcare data in the IoT process and structure is very sensitive and critical in terms of healthy and technical considerations. Outlier detection approaches are considered as principal tool or stage of any IoT system and are mainly categorized in statistical and probabilistic, clustering and classification-based outlier detection. Recently, fuzzy logic (FL) system is used in ensemble and cascade systems with other ML-based tools to enhance outlier detection performance but its limitation involves the false detection of outliers. In this paper, we propose a fuzzy logic system that uses the anomaly score of each point using local outlier factor (LOF), connectivity-based outlier factor (COF) and generalized LOF to eliminate the confusion in classifying points as outliers or inliers. Regarding human activity recognition (HAR) dataset, the FL achieved a value of 98.2 %. Compared to the performance of LOF, COF, and GLOF individually, the accuracy increased slightly, but the increase in precision and recall indicates an increase in correctly classified data and that neither true nor abnormal data is classified wrongly. The results show the increase in precision and recall which indicates an increase in correctly classified data. Thus, it can be confirmed that fuzzy logic with input of scores achieved the desired goal in terms of mitigating cases of false detection of anomalous data. By comparing the proposed ensemble of fuzzy logic and different types of local density scores in this study, the outcomes of fuzzy logic presents a new way of elaborating or fusing the different tools of the same purpose to enhance detection performance

Keywords: anomaly detection, outlier score, anomaly score, fuzzy logic, hybrid system

UDC 621

DOI: 10.15587/1729-4061.2023.274575

ANOMALY DETECTION IN INTERNET OF MEDICAL THINGS WITH ARTIFICIAL INTILLEGENCE

Shalau Farhad Hussein
College of Information Technology and Computer Science
Presidency of University of Kirkuk*

Zena Ez. Dallalbashi
Department of Electronic Technical Institute
Northern Technical University
Mosul, Iraq, 41002

Ahmed Burhan Mohammed
Corresponding author
College of Dentistry Presidency of University of Kirkuk*
E-mail: ahmedlogic79@uokirkuk.edu.iq

*University of Kirkuk
Al-Sayada Area Kirkuk, Kirkuk, Iraq, 36001

Received date 07.12.2022
Accepted date 15.02.2023
Published date 28.02.2023

How to Cite: *Hussein, S. F., Dallalbashi, Z. Ez., Mohammed, A. B. (2023). Anomaly detection in internet of medical things with artificial intillegence. Eastern-European Journal of Enterprise Technologies, 1 (4 (121)), 56–62. doi: https://doi.org/10.15587/1729-4061.2023.274575*

1. Introduction

Internet of things (IoT) becomes the most popular term in the recent advances in Healthcare devices. Whereas the most common example of IoT in health care is remote monitoring of patients, like IoT devices that collect patient data such as heart rate and biomarkers [1]. IoT devices offer new features for healthcare providers including accurate and in-time patient monitoring and treating. In addition, various wearable monitors and sensors provide plenty of benefits and capabilities for healthcare providers and their patients. Basically, the applications of IoT in the medical field are remote patient monitoring like biosignals, depression and mood monitoring and human activity recognition (HAR). Reliable IoT technology in the medical field requires proper data transmission and addressing critical security challenges [2].

Healthcare data is very sensitive and critical and any distortion or malfunction in the transmitter and receiver may change or contaminate the diagnosis of the patients. In cases of cyber-attacks or the noise of the equipment and the surrounding environment, there will be anomalies or outliers in this data. Those anomalies must be detected accurately in the real-time or appropriate moment to prevent any serious consequences, the worst of which is the life of the monitored patient. The concept of anomaly detection includes a wide range of applications, such as outlier or novelty detection and intrusion detection [3].

Outlier detection approaches are considered as principal tool or stage of any IoT system [2] and are mainly categorized in statistical and probabilistic, clustering and classification-based outlier detection. Statistical methods rely on previously measured data to approximate the correct behavior model of the data such as the autoregressive and moving average (ARMA) prediction model, adaptive kernel density estimator (AKDE) approach and classification and regression Trees (CART) model where new data is compared to the previously generated model data. If the results show the statistical significance of the data is different, the new data is marked as an anomaly. The probabilistic method relies on distinguishing outliers from normal or inlier data. If the probability is below a predetermined threshold, it is classified as abnormal. Outlier detection and classification during monitoring and detection of human activity using environmental sensors, wearable sensors, or both is still under development due to the prevalence and recent achievements in medical IoT and 6G era communications. Clustering-based outlier detection techniques or proximity-based method relies on the distances between the measured data to distinguish between outlier and inlier. Machine learning (ML)-based outlier detection is called usually a classification-based technique. Recently, the ensemble and cascade systems with other ML-based approaches were used to enhance outlier detection performance but its limitation involves the false detection of outliers [3]. Therefore, studies move forward to enhancing the ensemble approach for outlier detection that may decrease the false classification of outlier and increase performance accuracy.

2. Literature review and problem statement

The paper [4] addressed the most well-known algorithms based on data convergence as the local outlier factor (LOF), K-means algorithm, distributed LOF Computing algorithm (DLC), ellipsoidal neighborhood outlier factor (ENOF), connectivity-based outlier factor (COF) and Local Correlation Integral (LOCI). The paper emphasizes the powerful of LOF performance. Research [5] suggested local outlier factor that measures the relevance of data its surrounding neighbors. This research provided a detailed formal analysis showing that LOF has many desirable properties, and careful performance evaluation of the algorithm confirmed that the local outlier detection approach using local factor can be practical. The result shows a good ability to detect outliers with an accuracy more than 70 % but the main limitation is the misclassification of important data as outliers. Paper [6] applied compute unified device architecture (CUDA) to accelerate LOF. This paper showed a good increase in the performance in terms of elapsed time to examine the data with a 20 % time reduction compared with normal execution. Paper [7] investigated the connectivity-based outlier factor method. The experimental results show that Gaussian-COF and Laplacian-COF are more effective in detecting anomalous data with an accuracy more than 82 %. The limitation of the proposed approaches is the margins of neighbors. Paper [8] illustrated the outlier detection based on machine learning (ML) and artificial intelligence (AI) techniques that are developed for years to support the reliability of IoT, like support vector machine (SVM), logistic regression, K-nearest neighbors (KNN), tree-based methods and linear discriminant analysis (LDA). The paper [9] used one-class SVM (OCSVM) for outlier detection with an accuracy of 82.39 % but still suffers from the low performance. Research [10] used fuzzy logic to detect outliers and anomalous data based on specific fuzzy rules with an accuracy of 85 %. The main limit of this FL model is the missing and not addressed cases in the fuzzy rules. Research [11] used the FL system in ensemble system with other ML-based tools to enhance outlier detection performance, by using the FL stage to reduce the dataset size into features then using SVM for detection. The ensemble model showed an accuracy of 92.91 % because it has a narrow range of fuzzy rules to address. This model can be enhanced with a normalized value of FL inputs. In paper [12], FL is used in an ensemble system to evaluate many features of anomalous data, where the FL system uses Mahalanobis distance, fuzzy c-means (FCM), LOF, and Grubb test that indicates the presence of anomalies as inputs. This methodology leads to accuracy of 91.05 %. In this study, different ranges in FL's input are considered a challenge. In [13], authors proposed a two-stage cascaded OCSVM for water level monitoring system. In the first stage of the cascade model, OCSVM directly examine the (1–g) observation at a time point and detect the anomalies. In the second stage, OCSVM learns from n-gram feature vectors built on previous data to discover collective anomalies. Experimental results show that the proposed model can effectively detect anomalies and cluster anomalies with F1 score of 99 %. This study suffers from multi cascade steps that may leads latency in performance. Paper [14] proposed an anomaly detection method using cascade K-Means clustering and C4.5 decision tree method. The k-means clustering method is first used to split the training instances into k clusters using Euclidean distance similarity. The decision tree for each cluster adjusts the decision boundaries by learning the subgroups within the cluster. The proposed cascade model shows 95.8 % of accuracy and 95.6 % of precision. The decision tree model has a complicated architecture and is not easy to estimate anomaly score and use it with another approach within the same ensemble.

The cascade models for anomaly detection seem to be a reliable development either [13, 14]. They depend on assigning a score to each point to distinguish the anomalies within the data. The latest review [4] highlights the challenge of confusion in differentiating between critical status between outlier and inlier. This case of detection confusion varies among implemented algorithms and data structures. On the other hand, fuzzy logic is used as an aggregation tool to combine the results of many classical and ML-based tools in detecting outliers [12]. In contrast, the inputs for FL came from different approaches with different ways of detecting outliers. So, it's better to propose an FL system that uses inputs from different sources of anomaly detection tools but are similar in terms of outcome types and outlier scoring.

3. The aim and objectives of the study

This work aims to investigate the methodology of embedding different algorithms of outlier detection into one ensemble with fuzzy logic, where the input of FL will be more precise and comes from the same scoring models regarding anomaly detection models. Accordingly, this study comes to investigate the impact of local factor score on designing a decision-support system for anomaly detection.

To achieve this aim, the following objectives are accomplished:

– to propose a fuzzy system that uses the anomaly score of each point using LOF, COF and generalized LOF to eliminate the confusion in classifying points as outliers or inliers using the human activities dataset;

– to examine the proposed approach on the physical activity monitoring dataset;

– to compare the proposed approach with different modalities.

4. Materials and methods of research

4. 1. Objective and hypothesis of the study

The methodology in this study relies on obtaining data outliers within the local density and assign scores to outliers and inliers using LOF, COF and generalized local outlier factor (GLOF) methods then assign them as inputs to fuzzy logic. The proposed FL relies on three input scores, fuzzy inference mechanisms, and available fuzzy rules to discuss the state of available data scores and distinguish between complete/semi-outlier/inlier data. The actual advantage of replacing the direct evaluation of the LOF score with a fuzzy logic system is that it provides a mechanism to evaluate, decide and determine the exact state of small or confusing cases.

4. 2. Data collection

The human activity recognition (HAR) dataset includes continuous recordings of the human activities of 30 participants. The ages of participants range between 19 and 48 years. The recorded activities include 6 types like gait cycling (walking and walking upstairs/downstairs). The dataset contains 561 features estimated from the gyroscope and accelerometer recordings. The data set includes 10299 samples [15]. The time length of data differs according to activity types where standing/sitting/laying has 15 seconds time length and walking downstairs/upstairs has 12 seconds of signals. The HAR features are estimated using Body/Gravity/Body angular acceleration, jerk and magnitude.

The Physical Activity Monitoring (PAMAP2) dataset is built based on recordings of 18 different physical activities (gait cycling and movement: stand, lie, sit and walk; sport: run, Nordic walk, cycle, iron, rope jump and play soccer; daily activities: vacuum clean, ascend, descend stairs, watch TV, computer work, drive car, fold laundry and clean house) over 10 hours. The dataset is built using a heart rate monitor and inertial measurement units (IMUs) [16]. The recordings are built using 3 sensors on 3 different body positions. The first sensor is an IMU unit for a chest sensor fixation and the heart rate chest strap. The second IMU sensor is placed on the wrist, and the third IMU sensor is placed on the ankle.

4. 3. Estimating anomaly score using local outlier factor

The Local External Factor is an algorithm used to detect anomalies with an unsupervised approach. LOF differentiate between inlier and outlier by calculating the distance between the evaluated point and the local density of the field. LOF depends on the deviation of local density between examined point and its neighbors. So for each data point, the local density can be calculated by estimating the distances between close data points (k-nearest neighbors). Through these densities, normal and anomalous neighbors can be identified and detected, where the points with lower densities are outliers and vice versa. LOF procedure is summarized as follows [4].

First, for each point, there are k distances used to determine its k-nearest neighbors. K-distances are the distances between a point and its possible neighbors. The reachability distance refers to the maximum distance between two points and the k-distance for that point. The reachability distance is calculated for each k distance. As shown in (Fig. 1), O is the point in the center and $P1$ is a point close to it. The local reachability density (LRD) for that examined point is given by the following:

$$LRD_k(P1) = \frac{\sum_{B\in N_k(A)} reach-dist_k(P1,O)}{|N_k(A)|}, \quad (1)$$

where $reach-dist_k(P1,O)$ represent the reachability distances to all k-nearest neighbors of the point:

$$reach-dist_k(P1,O) = \max\{k-dist(O), d(P1,O)\}, \quad (2)$$

where d is the Euclidean distance.

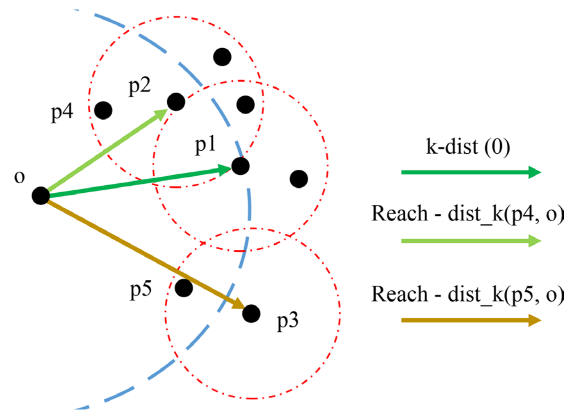

Fig. 1. Scattered points with different types of distances according to Local outlier factor method

The local reachability density refers to the density of the nearest points around a point that is calculated using all reachability distances for all k nearby points. The closer the points shows the lower distance and greater density. The final local outlier factor is calculated by the following:

$$LOF_k(P1) = \frac{\sum_{B\in N_k(A)} LRD_k(O)}{|N_k(A)| LRD_k(P1)}, \quad (3)$$

where the LOF expresses the mean ratio of the LRDs from k number of neighbors for a point O and the LRD for point $P1$.

4. 4. Estimating anomaly score using connectivity-based outlier factor

COF is an anomaly detection technique and an improved version of LOF technology. COF approach depends on assigning an anomaly score for each data point. A high COF score of point refers to the high probability of being an outlier. Basically, consider the spherical distribution of data points, but COF deals with a linear distribution. Briefly, the COF score of point $P1$ is calculated based on the distance function [17]:

$$COF(x) = \frac{dist(P1)}{\frac{1}{k}\sum_{j\in N_K(P1)} dist(j)}, \quad (4)$$

$$dist(P1) = \sum_{i=1}^{k} \frac{2(k+1-i)}{k(k+1)} dist(e_i), \quad (5)$$

where $dist(e_i)$ represents the ambient distance with edge points. Accordingly, the COF score equals the ratio mean distance of points x with its neighbors and the mean distance of x's neighbors' records which represents the chance to be an outlier.

4. 5. Estimating anomaly score using generalized local outlier factor

The GLOF measures the probability of point p being an outlier. GLOF uses the local density of point p and k-nearest neighbors to measure the likelihood of being an outlier. As a numerical value, if point p has a lower density than k-nearest neighbors, point p is more likely to be an outlier. Full mathematics and equations are described by [18]. The final estimated formula for the GLOF score of point p was expressed by the following:

$$GLOF_{MinPts}\left(p,x^1,x^2\right)= \\ =\frac{ard_{MinPts}\left(p,x^1\right)}{PM\left(\left\{ard_{MinPts}\left(j,x^1\right)\mid j\in N_{MinPts}\left(p\right)\right\},x^2\right)}, \quad (6)$$

where $PM(p, x)$ is the power means of point p with respect to x (arithmetic, geometric and harmonic means) and *ard* stands for the average reachability distance of point *p*.

4. 6. Anomaly detection using fuzzy logic

Fuzzy Logic is used as a decision support and validation tool by using the output of LOF, COF and GLOF. The purpose of FL is to re-classify points to outlier or inlier if one of the three outlier detection models has a different classification. Accordingly, the proposed FL system consists of three inputs and one output as shown in (Fig. 2). All programming and computational implementation are carried out using MATLAB with Fuzzy logic Toolbox (MathWorks, Natick, MA, United States) [19]. The programmatic implementation is carried on using a laptop with an i7-7300U CPU@ 1.90 GHz, 2494 MHz, 2 core(s) CPU Intel(R) core. A Mamdani type-FL is used to initialize the FL system, where the main components and stages of the FL structure are as follows.

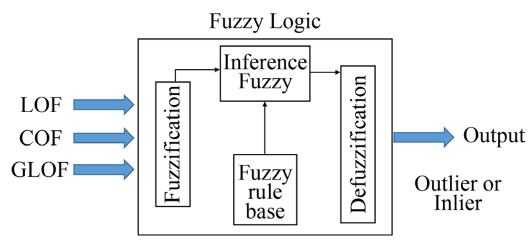

Fig. 2. Proposed fuzzy logic system for final evaluation

Fuzzification: It is used to convert three inputs (degree of being outlier or inlier) into fuzzy sets. The outputs of LOF, COF and GLOF represent the outlier score of each evaluated data. The output of each method is mapped between. The four membership functions of each input divide the input value into four main fuzzy sets using trapezoidal and triangle functions with the following labels: Completely Inlier (CI), Semi Inlier (SI), Semi Outlier (SO) and Completely Outlier (CO) as shown in (Fig. 3) for «LOF» input. The three inputs have the same membership structure and ranges after mapping their values. The output represents the final classification of data type using the same membership functions.

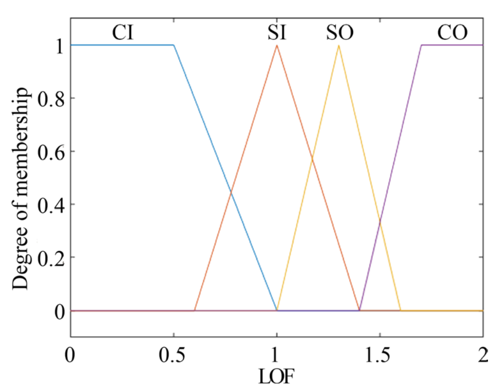

Fig. 3. Membership functions of input «LOF»

Rule base: It contains the set of and/or rules and the IF-THEN conditions that include the most occurred events and most cases based on input and prospective output. Mainly, the fuzzy rules address the different values of input or simply give a final decision (outlier or inlier) when facing different values from the three inputs. The fuzzy rules aim to eliminate the confusion of different outputs between LOF, COF and GLOF. The following fuzzy rules are samples of initialized fuzzy sets:

1. If LOF is CI and COF is CI and GLOF is CI then output is CI.
2. If LOF is CO and COF is CI and GLOF is CI then output is SO.
3. If LOF is SO and COF is CI and GLOF is CI then output is SI.

Inference engine: is responsible for processing and implementing the fuzzy rules numerically and getting the final fuzzy results. The processing contains implications from the antecedent to the consequent in rules then the aggregation of the consequents across the rules. FL parameters using MATLAB include «min» function as AND method, «max» function as OR method, «min» as implication function and «max» as aggregation method.

Defuzzification: this is the last step of the fuzzy inference system where we convert fuzzy results into original format or range (outlier or inlier). For the defuzzification process, the «centroid» that depends on the center of gravity is used.

4. 7. Evaluation metrics of detection performance

For an efficient the performance of anomaly detection approaches, various metrics is measured using true/false positive and true/false negative labels. The ground truth for anomaly data is determined by manual evaluation and annotation of outliers on a feature-by-feature basis. The three metrics are accuracy (ACC), recall (ReC) and precision (PRE):

$$accuracy=\frac{TP+TN}{TP+FP+TN+FN}, \quad (7)$$

$$recall=\frac{TP}{TP+FN}, \quad (8)$$

$$precision=\frac{TP}{TP+FP}, \quad (9)$$

where true positive (TP) refers to the correctly detected data as an outlier, false positive (FP) refers to the wrongly detected data as an inlier, true negative (TN) refers to the correctly detected data as an inlier, and false negative (FN) refers to the wrongly detected data as an outlier.

5. Results of fuzzy logic-based outlier detection

5. 1. FL-based outlier detection using human activity recognition dataset

The HAR data are evaluated using LOF, COF and GLOF separately and then the result of each model was used as input to the FL system. Outlier detection results show the ability to improve detection by significantly increasing both precision and recall with values of 92.5 % and 94 %, respectively (Fig. 4).

In terms of accuracy, the FL achieved a value of 98.2 %. Compared to the performance of LOF, COF, and GLOF individually, the accuracy increased slightly, but the increase in precision and recall (Fig. 4) indicates an increase in correctly classified data and that neither true nor abnormal data is classified wrongly. Thus, it can be confirmed that FL achieved the desired goal in terms of mitigating cases of false detection of anomalous data.

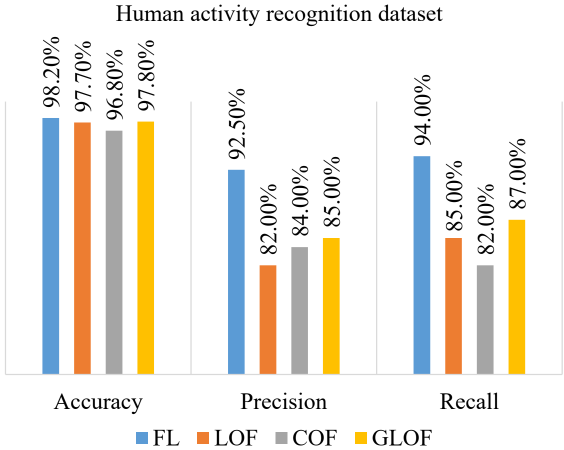

Fig. 4. Outlier detection using human activity recognition dataset

5. 2. FL-based outlier detection using physical activity monitoring dataset

The PAMAP2 data are evaluated using LOF, COF and GLOF separately and then the result of each model was used as input to the FL system. Outlier detection results in this type of data also showed the ability to improve detection by significantly increasing the accuracy, precision and recall with values of 88.2 %, 87.6 %, and 87 %, respectively (Fig. 5), where the comparison shows a significant increase in detection efficiency compared to the performance of LOF, COF, and GLOF individually, which did not exceed 83 %.

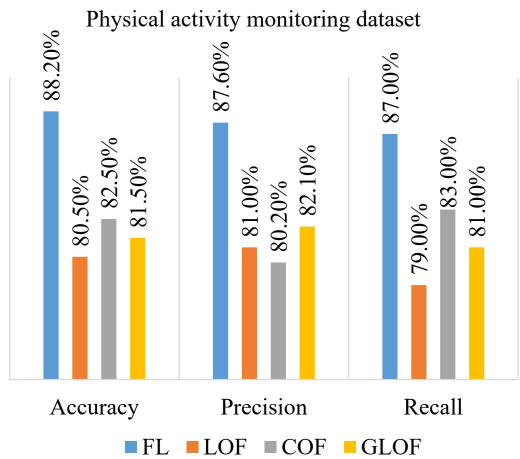

Fig. 5. Outlier detection using physical activity monitoring dataset

An increase in accuracy and other measures (Fig. 5) reflects the increase in the proportion of correctly classified data to the proportion of incorrectly classified data. The PAMAP2 data also show the ability of fuzzy logic to mitigate the error rate in detecting outliers by taking advantage of the score variance for each of the three primary methods.

5. 3. Comparison with different approaches

Based on related research work, including ML techniques based on data convergence in separating data using variable vector like OCSVM method [20] and Ramp loss based robust one-class SVM (ROCSVM) [21]. The results of the anomaly detection test in the HAR data show the ability of the proposed FL model to give better accuracy of 98.2 % (Fig. 6) because the fuzzy logic is able to take advantage of the varying anomaly score values resulting from LOF, COF and GLOF.

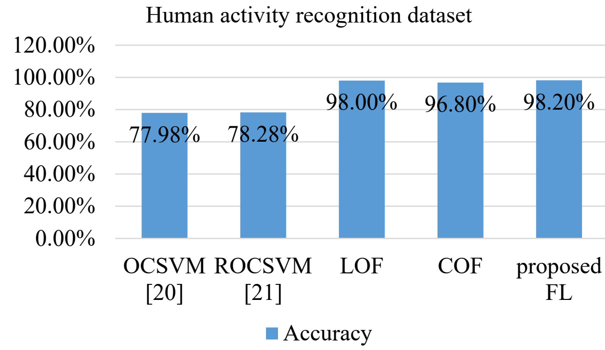

Fig. 6. Comparison of outlier detection accuracy with different approaches

This result reflects the ability of fuzzy logic to reduce or eliminate detection of misclassified or anomalous data by improving accuracy, precision, and search metrics of the dataset under investigation.

6. Discussion of the outlier detection results of the proposed system

Outlier detection and classification, during monitoring and recognition of human activities using ambient sensors, wearable sensors or both, are still under development and different methodologies as novel tools or ensembles of multi-approaches have been suggested [22]. The proposed methodology in this research depends on taking advantage of the data anomaly scores within the local density through the LOF, COF and GLOF methods between outlier and inlier and using them as an input for the fuzzy logic. The FL depends on the three input scores, the fuzzy inference mechanism and the available fuzzy rules to discuss the state of the available data score and distinguish between completely/semi outlier/inlier data. The actual benefit of replacing direct evaluation of the LOF score of the data with a fuzzy logic system that provides a mechanism for discussing and deciding the data to determine its exact state for small or confusing margins. Results provided using HAR data (Fig. 4) and PAMAP2 data (Fig. 5) show that fuzzy logic can achieve the expected goal by increasing the precision and recall values compared to the performance of each anomaly detection method individually. The methodology of using FL as an evaluation tool for the output score of mathematical methods shows a very promising method, where the use of this principle can be extended to include the output of available methods such as OCSVM and its new versions [20, 21] as FL input. Fuzzy logic can also be combined with improved neural network-based detection techniques [8]. Compared with [20, 21] (Fig. 6) ensemble of scoring models with FL showed a clear increase in accuracy from 78 % to 98 % which reflects the ability of fuzzy logic to reduce or eliminate detection of misclassified or anomalous data. The proposed method of elaborating FL with available anomaly metrics is considered as a new implementation of what was proposed in [11, 12] in terms of using fuzzy logic as an evaluation tool for outliers and anomalies in terms of using several parameters and measures as additional input for FL. The ensemble of OC-SVM, LOF, iForest and robust covariance estimation (RCE) has a reliable impact on detection accuracy with value of 97.18 % [23]. Compared with the proposed ensemble of fuzzy logic and different types of local density scores in this study with accuracy of 98.2 %, the fuzzy evaluation presents a new way of elaborating or merging the different tools of the same purpose to enhance detection performance. Compared with the usual implementation of FL using direct input like sensor recordings [10] or density- and distribution-based features [12], the proposed method presents more coherence features collection for FL and had a fixed range of values. In contrast, the only limitation of the proposed FL-based approach is the structure of membership functions and fuzzy rules which still need some improvement to address and handle some unpredicted conditions like critical scores and undefined ranges of values. The proposed work would be more efficient and applicable for datasets with numerical records because the fuzzy rules of this work depend on the data structure. Moreover, the score values of LOF, COF and GLOF may exceed the supposed numerical range and may lead to some problems with execution. Accordingly, fuzzy logic's input structure must be adapted based on analyzed data. Future work will include using some improved ML-based approaches to include more parameters as inputs and extending FL's membership structure and fuzzy rule set accordingly.

7. Conclusions

1. The proposed FL-based approach using the human activity detection dataset significantly improved both accuracy and recall with values of 92.5 % and 94 %, respectively, reaching an accuracy of 98.2 %, indicating that It shows the ability to improve outlier detection. The results show that fuzzy logic can achieve the expected goals by increasing precision and recall values compared to the performance of individual anomaly detection methods.

2. Regarding the physical activity monitoring dataset, outlier detection results for this type of data also showed the ability to improve detection by improving accuracy, precision and recall with values of 88.2 %, 87.6 % and 87 % showed.

3. This paper presents an ensemble approach using available tools to detect anomalies and outliers based on the local density principle, and refine the resulting anomaly scores as inputs to a fuzzy logic system. This result reflects the ability of fuzzy logic to reduce or eliminate misclassification or detection of anomalous data by improving accuracy, accuracy, and search metrics of the investigated data set.

Conflict of interest

The authors declare that they have no conflict of interest in relation to this research, whether financial, personal, authorship or otherwise, that could affect the research and its results presented in this paper.

Financing

The study was performed without financial support.

Data availability

Manuscript has no associated data.

References

1. Alsaydia, O. M., Saadallah, N. R., Malallah, F. L., AL-Adwany, M. A. S. (2021). Limiting COVID-19 infection by automatic remote face mask monitoring and detection using deep learning with IoT. Eastern-European Journal of Enterprise Technologies, 5 (2 (113)), 29–36. doi: https://doi.org/10.15587/1729-4061.2021.238359
2. Kadhim, K. T., Alsahlany, A. M., Wadi, S. M., Kadhum, H. T. (2020). An Overview of Patient's Health Status Monitoring System Based on Internet of Things (IoT). Wireless Personal Communications, 114 (3), 2235–2262. doi: https://doi.org/10.1007/s11277-020-07474-0
3. Samara, M. A., Bennis, I., Abouaissa, A., Lorenz, P. (2022). A Survey of Outlier Detection Techniques in IoT: Review and Classification. Journal of Sensor and Actuator Networks, 11 (1), 4. doi: https://doi.org/10.3390/jsan11010004
4. Alghushairy, O., Alsini, R., Soule, T., Ma, X. (2020). A Review of Local Outlier Factor Algorithms for Outlier Detection in Big Data Streams. Big Data and Cognitive Computing, 5 (1), 1. doi: https://doi.org/10.3390/bdcc5010001
5. Bzai, J., Alam, F., Dhafer, A., Bojović, M., Altowaijri, S. M., Niazi, I. K., Mehmood, R. (2022). Machine Learning-Enabled Internet of Things (IoT): Data, Applications, and Industry Perspective. Electronics, 11 (17), 2676. doi: https://doi.org/10.3390/electronics11172676
6. Razzak, I., Zafar, K., Imran, M., Xu, G. (2020). Randomized nonlinear one-class support vector machines with bounded loss function to detect of outliers for large scale IoT data. Future Generation Computer Systems, 112, 715–723. doi: https://doi.org/10.1016/j.future.2020.05.045
7. Vani, K., Neeralagi, R. R. (2017). IoT based health monitoring using fuzzy logic. International Journal of Computational Intelligence Research, 13 (10), 2419–2429. Available at: https://www.ripublication.com/ijcir17/ijcirv13n10_11.pdf
8. Bharathy, A. V., Basha, A. M. (2016). A hybrid intrusion detection system cascading support vector machine and fuzzy logic. World Applied Sciences Journal, 35 (1), 104–109.
9. Cateni, S., Colla, V., Vannucci, M. (2009). A fuzzy system for combining different outliers detection methods. 9th IASTED International Conference on Artificial Intelligence and Applications AIA 2009. Available at: https://www.researchgate.net/publication/235351913_A_Fuzzy_System_for_Combining_Different_Outliers_Detection_Methods

10. Tan, F. H. S., Park, J. R., Jung, K., Lee, J. S., Kang, D.-K. (2020). Cascade of One Class Classifiers for Water Level Anomaly Detection. Electronics, 9 (6), 1012. doi: https://doi.org/10.3390/electronics9061012
11. Muniyandi, A. P., Rajeswari, R., Rajaram, R. (2012). Network Anomaly Detection by Cascading K-Means Clustering and C4.5 Decision Tree algorithm. Procedia Engineering, 30, 174–182. doi: https://doi.org/10.1016/j.proeng.2012.01.849
12. Breunig, M. M., Kriegel, H.-P., Ng, R. T., Sander, J. (2000). LOF. ACM SIGMOD Record, 29 (2), 93–104. doi: https://doi.org/10.1145/335191.335388
13. Alshawabkeh, M., Jang, B., Kaeli, D. (2010). Accelerating the local outlier factor algorithm on a GPU for intrusion detection systems. Proceedings of the 3rd Workshop on General-Purpose Computation on Graphics Processing Units. doi: https://doi.org/10.1145/1735688.1735707
14. Wang, Y., Li, K., Gan, S. (2018). A Kernel Connectivity-based Outlier Factor Algorithm for Rare Data Detection in a Baking Process. IFAC-PapersOnLine, 51 (18), 297–302. doi: https://doi.org/10.1016/j.ifacol.2018.09.316
15. Anguita, D., Ghio, A., Oneto, L., Parra, X., Reyes-Ortiz, J. L. (2013). A public domain dataset for human activity recognition using smartphones. In Proceedings of the 21th international European symposium on artificial neural networks, computational intelligence and machine learning. Bruges. Available at: https://web.archive.org/web/20210506171341id_/https://www.elen.ucl.ac.be/Proceedings/esann/esannpdf/es2013-84.pdf
16. Reiss, A., Stricker, D. (2012). Introducing a New Benchmarked Dataset for Activity Monitoring. 2012 16th International Symposium on Wearable Computers. doi: https://doi.org/10.1109/iswc.2012.13
17. Pokrajac, D., Reljin, N., Pejcic, N., Lazarevic, A. (2008). Incremental Connectivity-Based Outlier Factor Algorithm. Electronic Workshops in Computing. doi: https://doi.org/10.14236/ewic/vocs2008.18
18. Jiang, S.-Y., Li, Q.-H., Li, K.-L., Wang, H., Meng, Z.-L. (2003). GLOF: a new approach for mining local outlier. Proceedings of the 2003 International Conference on Machine Learning and Cybernetics (IEEE Cat. No.03EX693). doi: https://doi.org/10.1109/icmlc.2003.1264462
19. Fuzzy Logic Toolbox. The MathWorks. Available at: https://www.mathworks.com/products/fuzzy-logic.html
20. Li, K.-L., Huang, H.-K., Tian, S.-F., Xu, W. (2003). Improving one-class SVM for anomaly detection. Proceedings of the 2003 International Conference on Machine Learning and Cybernetics (IEEE Cat. No.03EX693). doi: https://doi.org/10.1109/icmlc.2003.1260106
21. Xiao, Y., Wang, H., Xu, W. (2017). Ramp Loss based robust one-class SVM. Pattern Recognition Letters, 85, 15–20. doi: https://doi.org/10.1016/j.patrec.2016.11.016
22. Anderez, D. O., Lotfi, A., Pourabdollah, A. (2020). Eating and drinking gesture spotting and recognition using a novel adaptive segmentation technique and a gesture discrepancy measure. Expert Systems with Applications, 140, 112888. doi: https://doi.org/10.1016/j.eswa.2019.112888
23. Yahaya, S. W., Lotfi, A., Mahmud, M. (2019). A Consensus Novelty Detection Ensemble Approach for Anomaly Detection in Activities of Daily Living. Applied Soft Computing, 83, 105613. doi: https://doi.org/10.1016/j.asoc.2019.105613