2025 International Conference on Microwave, Optical, and Communication Engineering (ICMOCE) | 979-8-3315-6642-5/25/$31.00 ©2025 IEEE | DOI: 10.1109/ICMOCE64100.2025.11076747

A Two-Stage Anomaly Detection Framework for Improved Healthcare Using Support Vector Machines and Regression Models

Shreea Bose, Venkata Saketh Dakuri, Chittaranjan Hota, Senior Member, IEEE
Department of Computer Science, *BITS Pilani, Hyderabad Campus*, Hyderabad, India
{p20240026,f20220056,hota}@hyderabad.bits-pilani.ac.in

***Abstract*—This paper presents an effective two-stage anomaly detection technique for wireless body area networks (WBANs)-based personalized healthcare monitoring. Our method uses SMO regression (Sequential Minimal Optimization) for more in-depth contextual analysis and Support Vector Machines (SVM) for initial anomaly categorization. Domain-specific thresholds and sophisticated feature engineering are utilized to accurately identify point anomalies brought on by sensor noise or malfunctions and contextual anomalies resulting from interdependent physiological feature deviations. The robustness of the model is improved by features including heart rate discrepancies, rolling mean, and rolling standard deviation. With 99.61% and 99.97% detection accuracy for point and contextual anomalies, respectively, the model attains an overall accuracy of 99.59%. These findings highlight the promise of scalable, customized anomaly detection systems for WBAN-driven, real-time healthcare, which could lead to prompt treatments and better patient outcomes.**

***Index Terms*—SVM, SMO regression, WBANS, rolling mean, Anomaly detection**

I. Introduction

Wireless Body Area Networks (WBANs) have gained significant traction in healthcare and fitness monitoring, where real-time physiological data collection is crucial. These networks consist of wearable or implantable sensors that continuously track vital signs like heart rate, body temperature, blood oxygen levels, and electrocardiogram (ECG) readings. The primary goal of WBANs is to provide uninterrupted monitoring of an individual's health, enabling early detection of medical conditions, personalized healthcare, and emergency interventions.

Anomaly detection in WBANs is essential to distinguish between normal physiological variations and critical health issues. Identifying these anomalies can help detect irregular heart rhythms, early signs of diseases, or even sensor malfunctions that could otherwise lead to incorrect medical diagnoses. A point anomaly, Fig. 1, occurs when a single data point deviates from the expected range of values, irrespective of the surrounding context. An example could be a heart rate reading of 220 bpm in an adult under normal resting conditions. These are context-independent and are determined solely by the data

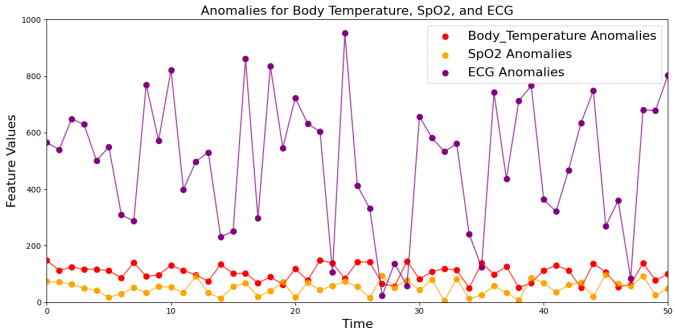

Fig. 1: Plot of Point Anomalies of WBAN features

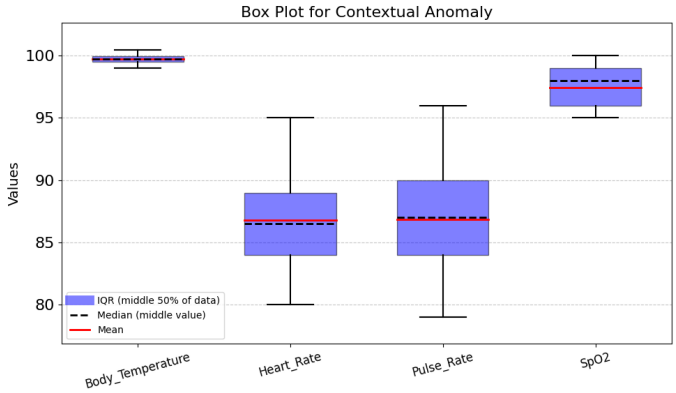

Fig. 2: Plot of Contextual Anomalies of WBAN features

point values compared to expected thresholds. A contextual anomaly, Fig. 2, occurs when a data point deviates from normal patterns given the specific context of the data in a WBAN. The same value may or may not be anomalous depending on contextual factors such as time, activity, or environmental conditions. The box plot summarizes data distribution using five key values: minimum, Q1, median, Q3, and maximum. According to the plot, we can say that Heart Rate and Pulse Rate are related contextually. This work presents a unique

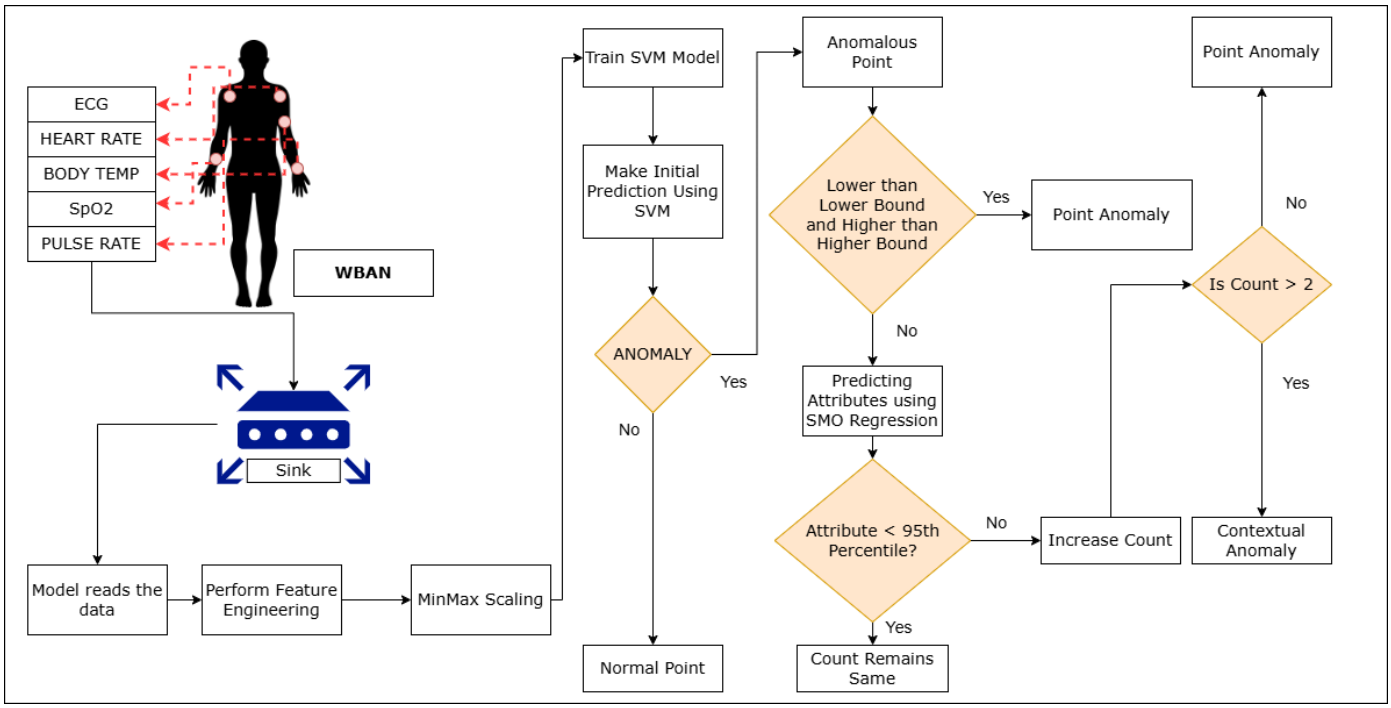

Fig. 3: The Two Stage Anomaly Detection System Flowchart

two-stage anomaly detection algorithm utilizing Wireless Body Area Network (WBAN) data for personalized healthcare, Fig. 3. The system combines Support Vector Machines (SVM) and SMO regression (Sequential Minimal Optimization) models to identify the point and contextual anomalies in health data. Support Vector Regression (SVR) and Sequential Minimal Optimization (SMO) are closely related because SMO is a practical approach for resolving the optimization problem in SVR. By decreasing prediction errors within a margin, SVR (optimized via SMO) is used in anomaly detection to model expected behavior and identify data points that drastically vary from this pattern as anomalies.

II. Background and Related Works

SMOReg, Gaussian Process, and Majority Voting (MV) algorithms were used in the study [1] to create an anomaly detection system for human physiological data. MV uses static criteria to check if the alarms are false or if there are actual medical issues. On the other hand, our approach supports dynamic thresholds by utilizing machine learning techniques. The two-tier method in [2] reduced latency and energy usage by avoiding cloud transmission and concentrated on anomaly detection at the Local Processing Unit (LPU) in WBANs. The study [3] used Physionet data to suggest an SVM-based anomaly detection model; however, it was limited in its capacity to adapt to dynamic settings due to its reliance on static thresholds. Using SMO regression, our model uses dynamic thresholds to overcome this constraint. [4] introduced a Logarithmic Kernel Function (LKF) for SVMs for better regression, providing better performance than conventional kernels. In [5], a Markov Model used RMSE to identify abnormalities, but our SMO-based method surpassed their results. While we used real-world data, [6] also investigated dynamic thresholding with SMO regression using synthetical anomalies. K-means and SMO were employed in hybrid models like [7] and [8]; however, they encountered parameter selection and performance constraints. Our method surpasses the current models in terms of accuracy and detection rates by merging contextual and point anomaly detection.

III. Model Architecture and Dataset

A. Dataset Used

The Dataset consists of 72,000 rows of time-series data from 16 persons over 5 days. Each individual's data was recorded thrice daily for five minutes, yielding 300 rows per session. Four people are defined as "patients" who display abnormal physiological patterns, and twelve are classified as "normal" in the dataset. Both contextual anomalies and point abnormalities are captured in the dataset. This configuration provides a thorough dataset to assess the efficacy of anomaly detection models by simulating real-world situations where physiological signals change due to different medical disorders. High-quality,

real-time physiological sensors were used to collect the data: the ECG AD8232 for EKG readings, the DFRobot heart rate sensor, the MAX30102 for SpO_2 and heart rate, and the MLX90614 for body temperature, Fig. 4. The participants were tracked by these Arduino-based sensors, which provided accurate physiological data for the anomaly detection model's training and testing.

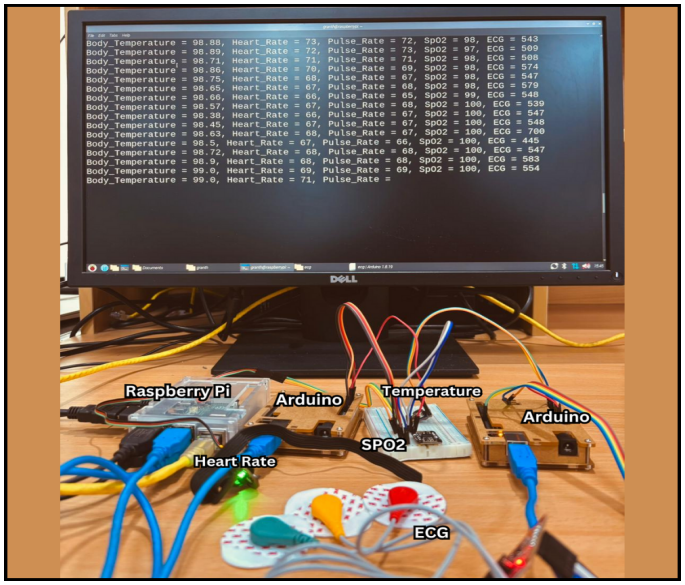

Fig. 4: IoT Testbed setup used to collect data

B. Proposed Model

Our two-stage anomaly detection framework begins by ingesting time-series health data from multiple IoT sensors and partitioning it by individual for subject-wise evaluation. In the preprocessing phase, we engineer key features, such as average heart rate, inter-sensor heart-rate differences, and rolling statistics of ECG readings, to capture both instantaneous and temporal signal characteristics. We then normalize all features using a MinMax scaler, ensuring uniform input scales for downstream models.

1) SVM for Identifying Anomalies: SVM allows non-linear separability in high-dimensional feature spaces by modeling the boundary between normal and anomalous classes using a kernel function in the context of anomaly detection. Because of its capacity to manage intricate, non-linear relationships in the data, the Radial Basis Function (RBF) kernel was selected for this application. The SVM initially classifies Test samples as normal (class 0) or abnormal (class 1).In the RBF equation, $K(x_i, x_j)$ is the kernel function between two data points x_i and x_j. γ is a parameter that defines the influence of a single training example (kernel width). $\|x_i - x_j\|^2$ is the squared Euclidean distance between x_i and x_j.

$$K(x_i, x_j) = \exp\left(-\gamma \|x_i - x_j\|^2\right) \tag{1}$$

2) Feature engineering and scaling: To ensure the characteristics fall within the same range, Min-Max scaling normalizes them before applying the SVM. This preprocessing step enhances the convergence and performance of the model. In Eq.(1) we calculate the average heart rate $\bar{H}_i$ using two measurements $H_{1,i}$ and $H_{2,i}$. The Eq.(2) computes the rolling mean $\mu_{v,t}$ of the ECG signal $\text{ECG}_{v,t-k}$ over a window size w. Eq.(3) calculates the rolling standard deviation $\sigma_{v,t}$ by measuring the deviation of $\text{ECG}_{v,t-k}$ from the rolling mean $\mu_{v,t}$ within the same window size w.

$$\bar{H}_i = \frac{H_{1,i} + H_{2,i}}{2} \tag{2}$$

$$\mu_{v,t} = \frac{1}{w} \sum_{k=0}^{w-1} \text{ECG}_{v,t-k} \tag{3}$$

$$\sigma_{v,t} = \sqrt{\frac{1}{w} \sum_{k=0}^{w-1} \left(\text{ECG}_{v,t-k} - \mu_{v,t}\right)^2} \tag{4}$$

3) Threshold–based Point Detection: In our anomaly-detection pipeline, the thresholding step serves as a fast, rule-based filter that flags any sample whose vital-sign measurements fall outside clinically plausible ranges. By defining lower and upper bounds (L_f, U_f) for each feature f (e.g. heart rate, temperature, SpO_2, ECG amplitude), we immediately detect "point anomalies" whenever even a single reading deviates beyond these physiological limits. Mathematically, for the ith test sample and feature set $\{f\}$, we set

$$\text{Anomaly}_i = \begin{cases} 1, & \exists f : \; X_{i,f} < L_f \;\vee\; X_{i,f} > U_f, \\ 0, & \text{otherwise.} \end{cases}$$

In this paper, we chose the default threshold values from Table I so that any sample with, for instance, a heart rate below 55 bpm or above 110 bpm is immediately marked anomalous before more sophisticated SVR-based checks are applied.

TABLE I: Physiological Thresholds for Point Anomaly Detection

Feature	**L**	**U**
Heart Rate (bpm)	55	110
Body Temperature (°F)	93	110
SpO_2 (%)	92	100
ECG Amplitude	450	700

4) Contextual Anomaly Detection using SVR: The second step involves training Support Vector Regression (SVR) models for every feature to determine baseline residuals. These residuals serve as detection criteria for contextual anomalies. The SVR models forecast expected feature values using all other features as input. Test samples beyond these levels are marked as contextual anomalies highlighting multi-feature deviations.

Algorithm 1 Anomaly Detection Using SVM and SVR Models with Threshold Checks

procedure ANOMALYDETECTION(input)
  1: Train SVM Model
  SVM_model $\leftarrow$ TrainSVM($X_{\text{train\_scaled}}, Y_{\text{train}}$)
  SVM_predictions $\leftarrow$ SVM_model($X_{\text{test\_scaled}}$)
  2: Compute Baseline Residuals with SVR
  $e_{i,f} \leftarrow \left|\text{SVR}_f(X_{\text{train\_scaled},-f}) - X_{\text{train\_scaled},i,f}\right|$
  baseline_residual$_f \leftarrow$ Percentile$_{95}(\{e_{i,f}\})$
  3: Threshold–based Point Detection
  Define physiological ranges: HR, Temp, SpO_2, ECG
  for each test sample i **do**
    if any $X_{\text{test},i,f}$ outside its range **then**
      Anomaly$_i \leftarrow 1$ *// Point anomaly*
  4: SVR-based Contextual Detection
  for each remaining i not flagged **do**
    $v_i \leftarrow 0$
    for each feature f **do**
      $\hat{x}_{i,f} \leftarrow \text{SVR}_f(X_{\text{test\_scaled},i,-f})$
      $e_{i,f} \leftarrow \left|\hat{x}_{i,f} - X_{\text{test\_scaled},i,f}\right|$
      if $e_{i,f} >$ baseline_residual$_f$ **then**
        $v_i \leftarrow v_i + 1$
    if $v_i \geq 2$ **then**
      Anomaly$_i \leftarrow 2$ *// Contextual anomaly*
    else
      Anomaly$_i \leftarrow 0$ *// No anomaly*
  return Anomaly(output)

In Algorithm I, the first stage, a support-vector classifier (SVC) flags potential anomalies. Feature-specific thresholds are applied post-training to outright remove point anomalies, such as samples breaching predefined physiological limits (e.g., heart rate $<$ 55 bpm or heart rate $>$ 110). In the second stage, we isolate remaining SVC-flagged samples and apply per-feature support-vector regressors to estimate expected measurements, computing residuals against empirically determined 95th-percentile baselines. Samples exceeding these residual thresholds in multiple features are labeled as contextual anomalies. This hierarchical approach combines robust global classification with fine-grained, feature-level validation to achieve high detection accuracy and zero missed anomalies.

IV. EXPERIMENTAL RESULTS AND DISCUSSION

Our model performs quite well on the test set, properly classifying 7,200 anomalies and 10,726 normal cases, demonstrating its remarkable ability to discriminate between anomalous and healthy signals. Table II shows that there are zero false negatives, indicating that every actual anomaly was properly discovered, and only 74 false positives, or normal signals that were mistakenly flagged as anomalies.

TABLE II: Confusion Matrix for Support Vector Classifier

		Predicted	
		Non-Anomalous	**Anomalous**
Actual	**Non-Anomalous**	10726	74
	Anomalous	0	7200

The suggested anomaly detection system integrates machine learning approaches with domain expertise to detect point and contextual anomalies effectively. Fig. 5 shows the predicted anomalies and original anomalies of the features collected from WBANs. We can see that most predicted anomalies are overly concentrated on the original anomalies, showing that our model works well.

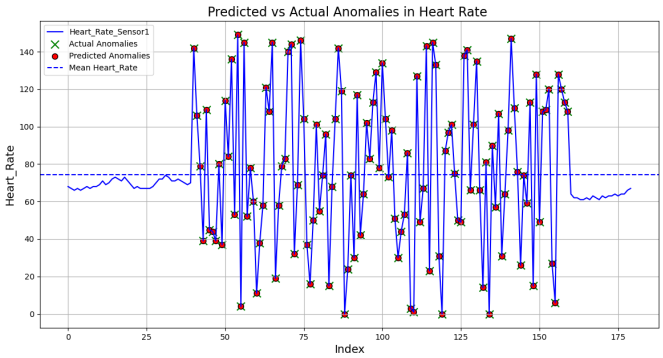

Fig. 5: Predicted vs Original Anomalies

Our model performs exceptionally well on various evaluation metrics, surpassing baseline techniques, Fig. 6. With an overall anomaly detection accuracy of **99.59%**, the model significantly outperforms DBSCAN with KMeans (60.01%), SVM (69.29%), and linear regression (60.00%). Significantly lower than baseline models like SVM (0.3071) and DBSCAN with KMeans (0.3999), the mean absolute error (MAE) is 0.0041. With an overall accuracy of 100% the precision, recall, and F1-score for both the anomalous and normal classes also surpass 99%. With an accuracy of **99.61%** for point anomalies and **99.97%** for contextual anomalies, the model demonstrates exceptional anomaly identification granularity and robustness in detecting localized and associated patterns.

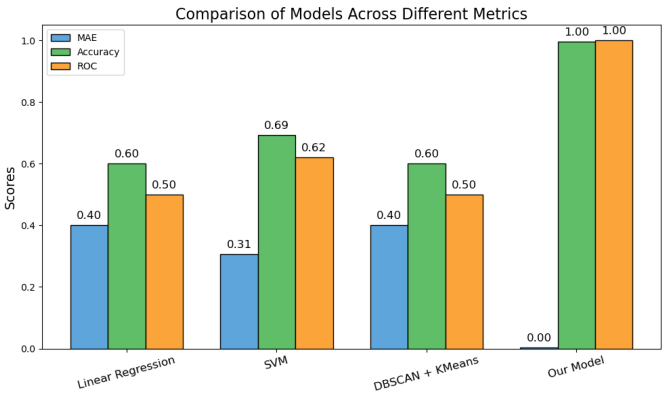

Fig. 6: Comparision of Accuracy, MAE and ROC

Model	Precision	Recall	F1-Score	Accuracy	Time (s)	Latency (ms)
Our Model	0.9928	0.9993	0.9961	0.9968	6.573	0.003
RF	0.9924	0.9994	0.9959	0.9967	20.857	0.016
FFNN	0.9924	0.9993	0.9958	0.9967	87.204	1.010
GRU	0.9921	0.9993	0.9957	0.9966	104.903	1.239

TABLE III: Comparison of Our Model with Deep Learning Models

From an IoT perspective, our two-stage anomaly detection model offers clear advantages over Deep Learning models, Table III. While all variants achieve very high accuracy (0.996–0.997), our SVR-based pipeline delivers the highest precision (0.993) with the lowest total runtime (6.57 s) and minimal per-sample latency (0.003 ms). In contrast, the Random Forest, feed-forward neural network (FFNN), and GRU models require 3–16× more computation time and incur per-sample delays over 0.01 ms, which can quickly deplete resources on constrained edge devices. High precision ensures that false alarms remain rare—a critical requirement when battery-powered sensors transmit alerts over limited bandwidth—while low latency guarantees near-real-time response to health anomalies. Thus, even with comparable accuracy, the SVR variant is better suited for real-world IoT deployments where energy efficiency, fast inference, and reliability are dominant. Fig. 7 shows the total end-to-end runtime for each anomaly-detection variant on the test set, highlighting that our model completes inference in just 6.57 s, substantially faster than RF (20.86 s), FFNN (87.20 s), and GRU (104.90 s).

Conclusion

The two-stage anomaly detection methodology presented in this paper uses Support Vector Machines (SVM) and Support Vector Regression (SVR) to detect contextual and point anomalies in physiological data. The suggested method successfully separates physiologically significant patterns from sensor noise by combining machine learning approaches with domain-specific thresholding, improving detection reliability. The proposed approach achieved detection accuracies of 99.61% and 99.97% for point and contextual anomalies, respectively, resulting in an overall anomaly detection accuracy of 99.59%. A mean absolute error of 0.0041 further demonstrates the remarkable precision attained by our approach. The model, created as a scalable solution for real-time physiological health monitoring, may be applied to various healthcare applications because it incorporates customized thresholds, guaranteeing personalized detection based on distinct user profiles.

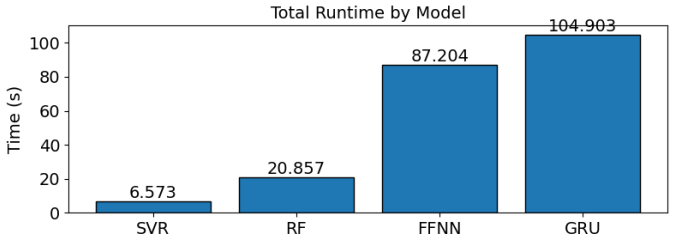

Fig. 7: Comparison of Run-time with Deep Learning Models

References

[1] M. U. Harun Al Rasyid, F. Setiawan, I. U. Nadhori, A. Sudarsonc, and N. Tamami, "Anomalous data detection in wban measurements," in *2018 International Electronics Symposium on Knowledge Creation and Intelligent Computing (IES-KCIC)*, 2018, pp. 303–309.

[2] S. Jain, P. Jain, P. Upadhyay, J. Moualeu, and A. Srivastava, "An energy efficient health monitoring approach with wireless body area networks," *ACM Transactions on Computing for Healthcare*, vol. 3, no. 3, p. 1–22, Apr 2022.

[3] O. Salem, A. Guerassimov, A. Mehaoua, A. Marcus, and B. Furht, "Anomaly detection in medical wireless sensor networks using SVM and linear regression models," *Int. J. E-health Med. Commun.*, vol. 5, no. 1, pp. 20–45, Jan. 2014.

[4] B. Hicdurmaz, N. Calik, and S. Ustebay, "Gauss-like logarithmic kernel function to improve the performance of kernel machines on the small datasets," *Pattern Recognition Letters*, vol. 179, pp. 178–184, 2024. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S016786552400014X

[5] M. U. Harun Al Rasyid, I. U. Nadhori, I. Syarif, I. Winarno, F. Furoida, and A. Amrullah, "Anomaly detection in wireless body area network using mahalanobis distance and sequential minimal optimization regression," in *2021 International Seminar on Application for Technology of Information and Communication (iSemantic)*, 2021, pp. 64–69.

[6] S. A. Haque, M. Rahman, and S. M. Aziz, "Sensor anomaly detection in wireless sensor networks for healthcare," *Sensors (Basel)*, vol. 15, no. 4, pp. 8764–8786, Apr. 2015.

[7] U. Rashid, M. F. Saleem, S. Rasool, A. Abdullah, H. Mustafa, and A. Iqbal, "Anomaly detection using clustering (k-means with dbscan) and smo," *Journal of Computing and Biomedical Informatics*, vol. 7, no. 02, Sep. 2024. [Online]. Available: https://jcbi.org/index.php/Main/article/view/598

[8] S. Gadal, R. Mokhtar, M. Abdelhaq, R. Alsaqour, E. S. Ali, and R. Saeed, "Machine learning-based anomaly detection using k-mean array and sequential minimal optimization," *Electronics*, vol. 11, no. 14, 2022. [Online]. Available: https://www.mdpi.com/2079-9292/11/14/2158