Shapelet Transformation of Multivariate Time Series for IoT Anomaly Detection

Wahyuddin S.
Department of Informatics, Institut Teknologi Sepuluh Nopember, Surabaya, Indonesia
7025231009@student.its.ac.id

Ahmad Saikhu
Department of Informatics, Institut Teknologi Sepuluh Nopember, Surabaya, Indonesia
saikhu@its.ac.id (corresponding author)

Agus Budi Raharjo
Department of Informatics, Institut Teknologi Sepuluh Nopember, Surabaya, Indonesia
agus.budi@its.ac.id

Received: 19 December 2025 | Revised: 28 January 2026 and 5 February 2026 | Accepted: 7 February 2026

 DOI: https://doi.org/10.48084/etasr.17048

ABSTRACT

The proliferation of Internet of Things (IoT) devices has generated substantial volumes of multivariate time-series data in multiple domains. Such data are susceptible to anomalies that may indicate system malfunctions or security threats. This research introduces a novel shapelet transformation approach for classifying multivariate time-series data to improve anomaly detection in IoT systems. Our approach distinguishes itself from the classic Shapelet Transform by specifically optimizing the extraction process to handle high-dimensional IoT data more efficiently, contrasting with methods such as Fast Shapelets, which are primarily designed for speed without focusing on multivariate contexts. This methodology centers on extracting short, informative subsequences, known as shapelets, from time series to facilitate classification. This approach is validated using the industrial IoT fault detection dataset for predictive maintenance in automation, which contains 1,000 entries of sensor data collected from machines in an industrial automation environment. This dataset includes three main sensor measurements: vibration (mm/s), temperature (°C), and pressure (Bar). The evaluation process involves partitioning the data into training and test sets and employing cross-validation to ensure robustness. The performance of the proposed method is benchmarked against traditional algorithms. Results demonstrate notable improvements: the F1-score is 0.6451 for temperature, 0.5778 for vibration, and 0.6984 for pressure, with an overall accuracy of 94%. This study establishes a framework for enhancing IoT system reliability by advancing anomaly detection, data mining, and machine learning.

Keywords-shapelet transformation; classification; multivariate; time series; anomaly detection

I. INTRODUCTION

The Internet of Things (IoT) enables widespread data exchange by connecting devices across domains such as smart cities, healthcare, industrial automation, and environmental monitoring. However, the resulting multivariate time-series data present challenges for timely and effective anomaly detection. Addressing these challenges is essential for reliable IoT operations [1].

Anomalies in IoT systems can result from sensor failures, environmental fluctuations, or cyberattacks, potentially causing disruptions or critical system failures. Consequently, timely detection and response to anomalies are vital for maintaining IoT system integrity. Traditional anomaly detection methods, which often rely on statistical techniques or heuristics, often struggle to handle the complexity and high dimensionality of IoT data [2, 3].

Recent advancements in machine learning and data mining have facilitated the development of sophisticated anomaly detection techniques that leverage time-based patterns in time series data. Among these innovative approaches, shapelet-based methods are particularly noteworthy due to their capacity to extract features that are both interpretable and effective in identifying anomalies [4]. Shapelets, which are short, unique parts of a time series, highlight key patterns for classification and help spot local anomalies that larger models might miss. Turning time series data into a shapelet-based feature space helps classification systems focus on what matters most, making models more accurate and transparent [5]. This

approach has become more popular as real-time decision-making becomes necessary.

Earlier work mostly focused on single-variable time series and standard outlier detection. As IoT systems have grown, research has increasingly focused on multivariate time series, underscoring the need to examine complex links among variables. For example, authors in [6] proposed a statistical framework for detecting anomalies in multivariate time series and highlighted flaws in older methods, whereas authors in [7] proposed a multiview unsupervised shapelet learning framework for clustering multivariate time series.

Advancements in machine learning have significantly influenced anomaly detection methodologies. Studies have demonstrated that deep learning models, including Recurrent Neural Networks (RNNs) and Long Short-Term Memory (LSTM) networks, can identify anomalies by learning temporal patterns, thereby improving detection accuracy. However, these models typically require extensive labeled datasets, which are often unavailable in practical IoT environments because of privacy concerns [8]. A hybrid Convolutional Neural Network (CNN)–RNN–LSTM model was introduced to enhance time series–based intrusion detection through integrated spatial and temporal pattern learning. This method aligns with studies on Shapelet Transformation for IoT anomaly detection, highlighting the importance of robust and interpretable temporal features [9].

Although shapelet-based methods have improved the classification of time-based data, their use for finding unusual patterns in IoT data with multiple variables remains limited. Most research focuses on classifying data rather than directly detecting anomalous behavior, which is key to the safety of IoT systems. Some studies use deep learning to spot anomalies, but shapelet transformation has not been widely tried in this area [10]. Shapelet transformation is interpretable and captures important features, but many methods have not been tested on real IoT data. This study aims to fill these gaps by creating a shapelet-based approach for classifying and identifying unusual patterns in multivariate IoT data to improve the accuracy and reliability of IoT systems [11].

This research proposes a shapelet transformation approach for classifying multivariate time series, with a focus on anomaly detection in IoT systems. The methodology comprises two main parts: extracting shapelets and using them in a classifier to detect anomalies. This approach is anticipated to surpass traditional techniques by providing a more robust classification framework. The proposed method is evaluated on real-world IoT datasets, compared with baseline models, and assessed using metrics such as accuracy, precision, recall, and F1-score. The findings aim to advance IoT anomaly detection research and offer practical guidance for implementing shapelet-based solutions.

II. RESEARCH METHODOLOGY

A. Data Collection

The shapelet transformation approach was evaluated using the publicly available Industrial IoT Fault Detection Dataset for Predictive Maintenance in Automation. This dataset contains 1,000 entries of sensor data collected from machinery operating in an industrial automation environment. It includes three primary sensor measurements: vibration (mm/s), temperature (°C), and pressure (Bar), which are critical for monitoring industrial equipment health. Two additional derived features, Root Mean Square (RMS) vibration and mean temperature, support the classification of potential faults [12]. Each entry provides a multivariate time series with varying lengths and sampling rates, representing both normal and abnormal operational states. The dataset was first cleaned to ensure consistency and to address missing values, which is necessary for robust analysis. The Damage Label column categorizes equipment condition into three groups: 0 for No Fault, 1 for Bearing Fault, and 2 for Overheating. The dataset is publicly available on Kaggle and can be used for data exploration, feature engineering, and model development. The data can be accessed at: https://www.kaggle.com/datasets/ziya07/industrial-iot-fault-detection-dataset.

As shown in Figure 1, pairwise multivariate feature relationships in IoT sensor data demonstrate class separability across vibration, temperature, and pressure dimensions. Each point corresponds to a time-series segment labeled by fault type (0 = No Fault, 1 = Bearing Fault, 2 = Overheating). The diagonal plots display the marginal distributions of each feature, whereas the off-diagonal scatterplots illustrate inter-feature dependencies. Table I presents the accuracy metric, which quantifies the overall correctness of the model's predictions and remains consistently high at 0.98 for all three sensor data types. This result demonstrates that the model accurately classifies the majority of instances across different sensor modalities. The precision metric, representing the proportion of true positives among all positive predictions, is also consistently 1.00, indicating highly accurate identification of positive instances with minimal false positives.

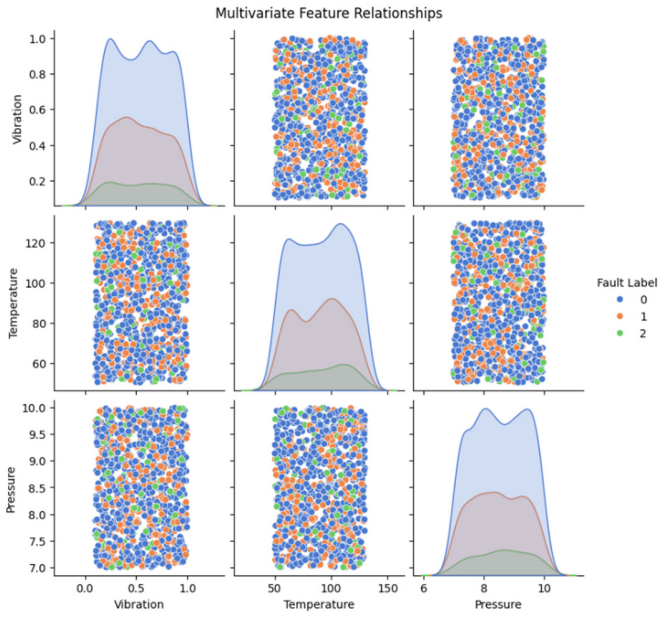

Fig. 1. Multivariate feature relationships.

TABLE I. PERFORMANCE METRICS OF INDIVIDUAL SENSOR FEATURES FOR ANOMALY DETECTION

Sensor	Accuracy	Precision	Recall	F1-score
Temperature	0.98	1.00	0.46	0.63
Vibration	0.98	1.00	0.39	0.56
Pressure	0.98	1.00	0.34	0.51

In contrast, the recall metric, which measures the proportion of true positives among all actual positives, exhibits greater variability across sensor data types: 0.46 for temperature, 0.39 for vibration, and 0.34 for pressure. These results indicate that the model fails to identify a substantial number of positive instances, particularly in the pressure and vibration datasets. The F1-score, calculated as the harmonic mean of precision and recall, provides a balanced assessment of model performance, with values of 0.63 for temperature, 0.56 for vibration, and 0.51 for pressure, reflecting the trade-off between precision and recall for each sensor type.

Figure 2 presents a low-dimensional visualization (PCA/t-SNE) of latent representations learned from multivariate IoT time series. Compared to the raw feature space, the transformed representations exhibit improved class separability, demonstrating the effectiveness of the shapelet-based transformation in capturing discriminative temporal patterns for anomaly detection.

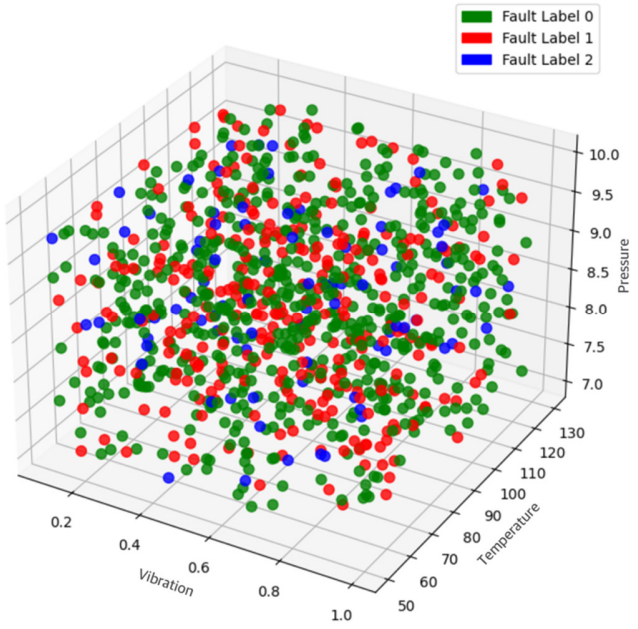

Fig. 2. 3D scatter plot of sensor data by fault label.

B. Shapelet Extraction

We use a shapelet transformation to find and classify unusual behavior in complex IoT data. First, we prepare the data by making them complete and even; missing values are imputed, and all data are standardized for training. The data are then divided into training and test sets using a method that maintains a balanced class distribution, which helps assess the model's performance [13].

Figure 3 depicts the main components of the IoT fault detection system: the Industrial IoT Fault Detection Dataset, Data Analysis, and Shapelet Transformation. The dataset comprises sensor data, including temperature, vibration, and pressure, used for anomaly detection. During the Data Analysis phase, the system collects and preprocesses the data, including cleaning and transformation, to prepare it for shapelet extraction.

In the Shapelet Transformation stage, the algorithm identifies significant subsequences within the time series. The system measures the similarity between new data and the shapelets, then uses a threshold to determine whether the new data are abnormal. If the input data exceed this threshold, the system flags issues within the IoT environment.

The framework uses the Shapelet Transform Classifier to find shapelet subsequences that best represent each class in the data. This helps the model capture temporal trends and differences that indicate anomalies. The classifier learns to recognize each class's distinguishing features from labeled training data. Shapelet selection uses criteria that prioritize subsequences with meaningful patterns and robustness across contexts. Shapelet lengths are set by assessing data variability and balancing specificity with generality. An information-gain-based quality metric ensures that the selected shapelets are highly discriminative, thereby significantly improving classification performance [14].

Algorithm 1 FindBestShapelet(T, min, max)
Where T is a set of time series
$best\_quality$, $quality$
$best\_shapelet$, $shapelet$
for T_i in T **do**
 for $l = min$ **to** max **do**
  for $p = 0$ **to** $|T_i| - l + 1$ **do**
   $shapelet = T_{i,p}^{l}$
   $quality =$ checkCandidate (T, $shapelet$)
   if $quality > best\_quality$ **then**
    $best\_quality = quality$
    $best\_shapelet = shapelet$
return $best\_shapelet$

The "FindBestShapelet" algorithm (Algorithm 1) receives as input a set of time series data (T) along with the minimum and maximum shapelet lengths (min and max, respectively). It iterates through each time series (T_i) in T and examines all possible subsequences of length l, where l ranges from min to max. For each subsequence, the algorithm extracts a candidate shapelet ($shapelet = T_{i,p}^{l}$) and evaluates its quality using the checkCandidate function. If the quality of the current shapelet exceeds the best quality found so far, the algorithm updates both the best quality and the best shapelet. After training, the model is evaluated using a confusion matrix and classification report, which provide accuracy, precision, recall, and F1-score. This framework enables faster and more effective anomaly detection in IoT systems.

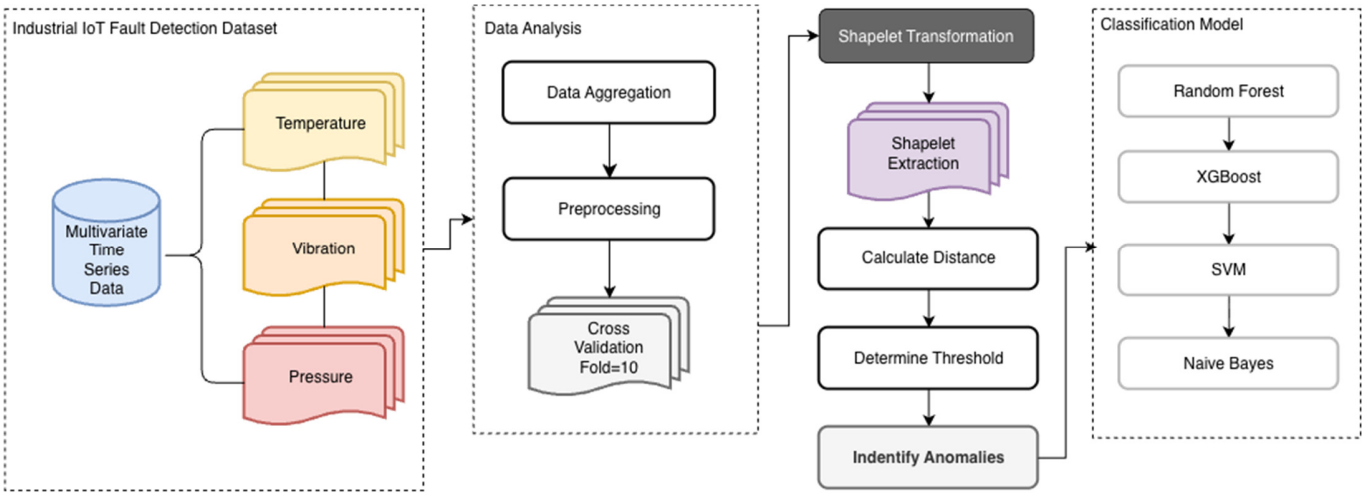

Fig. 3. Overall architecture for IoT anomaly detection.

C. Classification Framework

The experimental framework in this study is designed to align with and extend prior research in multivariate time-series classification and anomaly detection for IoT systems. Existing studies primarily rely on feature-based classifiers, ensemble learning, and boosting methods. Accordingly, baseline models such as Naive Bayes, Support Vector Machines (SVM), Random Forest, and XGBoost are incorporated to represent these commonly adopted approaches.

In contrast, the proposed framework introduces a shapelet transformation stage to explicitly capture localized temporal patterns, which have been identified in recent literature as critical for effective anomaly detection [15]. By transforming raw multivariate sensor data into a shapelet-based feature space, the proposed method bridges conventional classification techniques with interpretable subsequence-based learning. This alignment ensures a fair comparison with established methods while clearly highlighting the methodological contribution of the proposed approach. Table II summarizes the alignment between categories of related work and components of the proposed framework.

TABLE II. ALIGNMENT OF RELATED WORK CATEGORIES WITH FRAMEWORK COMPONENTS

Related work category	Representative methods	Framework component
Feature-based classifiers	Naive Bayes, SVM	Baseline classification path
Ensemble learning	Random Forest	Baseline classification path
Boosting methods	XGBoost	Baseline classification path
Subsequence-based learning	Shapelets	Shapelet extraction & transformation
Interpretable anomaly detection	Shapelets visualization	Shapelet-based classification

Motivated by the limitations of global feature-based and ensemble models identified in prior studies, this work adopts a shapelet-based transformation framework to explicitly capture localized temporal patterns, enabling improved anomaly detection performance and interpretability in industrial IoT systems.

D. Anomaly Detection

The classification framework is designed to identify anomalies within IoT data. Anomalies are detected based on classification outcomes, with instances labeled as anomalous flagged for further analysis. A thresholding mechanism controls the sensitivity of the anomaly detection process, enabling adjustment of the false-positive and false-negative rates to meet application-specific requirements.

E. Evaluation Metrics

To assess the effectiveness of the proposed shapelet transformation approach, several performance metrics commonly used in anomaly detection tasks are utilized:

$$\text{Accuracy} = \frac{TP+TN}{TP+FP+TN+FN} \quad (1)$$

$$\text{Precision} = \frac{TP}{TP+FP} \quad (2)$$

$$\text{Recall} = \frac{TP}{TP+FN} \quad (3)$$

$$\text{F1} - \text{score} = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}} \quad (4)$$

These metrics provide a comprehensive evaluation of the model's performance, enabling effective assessment of its ability to accurately identify anomalies while minimizing false positives and false negatives. The Area Under the Receiver Operating Characteristic (ROC) Curve (AUC) is also considered to evaluate the model's overall discrimination ability.

III. RESULTS AND DISCUSSION

The experimental results confirm the effectiveness of the proposed shapelet transformation approach for detecting anomalies in multivariate time-series data generated by industrial IoT systems. The evaluation was performed using the Industrial IoT Fault Detection Dataset, which contains real-world sensor measurements collected from industrial environments. The proposed method was benchmarked against

several widely used classification algorithms, including SVM, Random Forest, XGBoost, and Naive Bayes.

A. Performance Metrics

To provide a quantitative comparison between the proposed shapelet transformation approach and baseline classifiers, several standard performance metrics were employed. These metrics include accuracy, precision, recall, F1-score, and AUC, which collectively offer a comprehensive assessment of classification effectiveness, particularly for anomaly detection tasks in industrial IoT environments. As shown in Figure 4, the proposed shapelet transformation approach achieves the highest performance across all evaluation metrics, particularly in terms of accuracy, F1-score, and AUC. This demonstrates its superior capability in capturing discriminative temporal patterns for anomaly detection in industrial IoT systems compared to conventional baseline classifiers.

B. Cross-Validation Analysis

Cross-validation was performed to assess model stability and robustness. Figure 5 presents the results over 10 folds for accuracy, precision, recall, and F1-score.

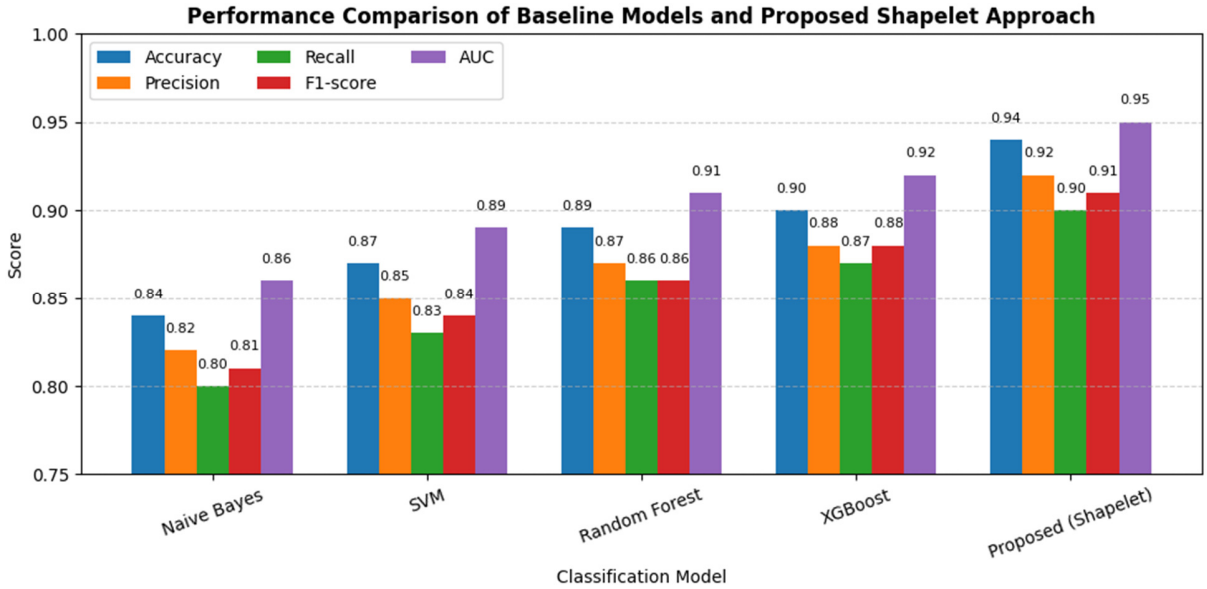

Fig. 4. Performance comparison of baseline models and the proposed shapelet approach.

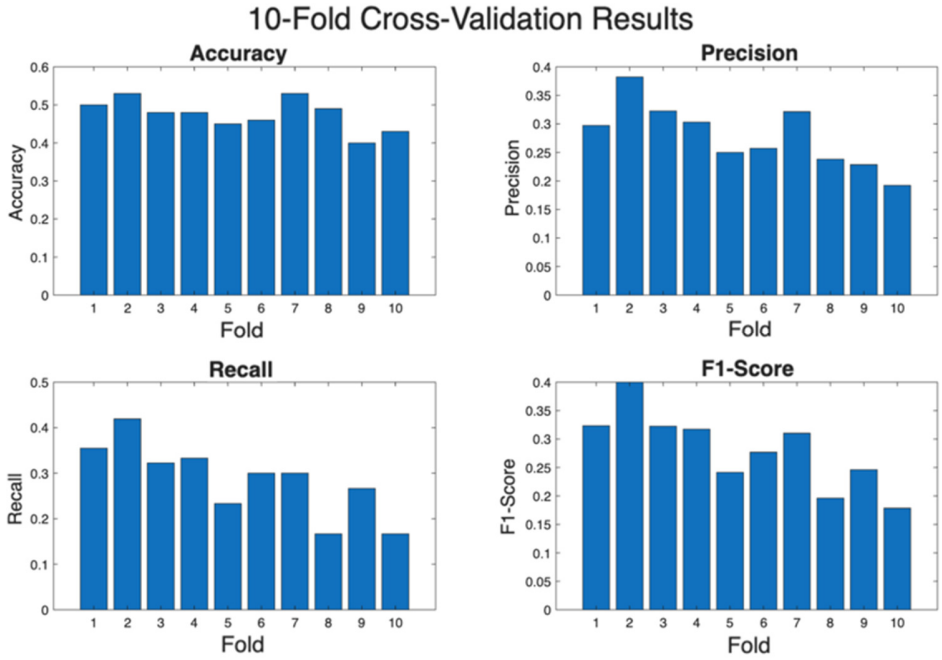

Fig. 5. Evaluation results of cross-validation for anomaly detection classification.

As shown in Figure 5, accuracy ranges from approximately 0.35 to 0.45. The precision graph demonstrates effectiveness in identifying positive instances, with values ranging from 0.15 to 0.30. The recall graph reflects sensitivity, representing the proportion of true positives correctly identified, ranging from 0.15 to 0.45. The F1-score graph combines precision and recall to provide a balanced assessment of overall performance, with values spanning 0.15 to 0.35. These results illustrate the model's consistency and sensitivity in identifying anomalous instances across different subsets of the dataset.

C. Shapelet Feature Visualization

Figures 6–8 show example shapelets from each sensor, highlighting the key patterns used for anomaly detection.

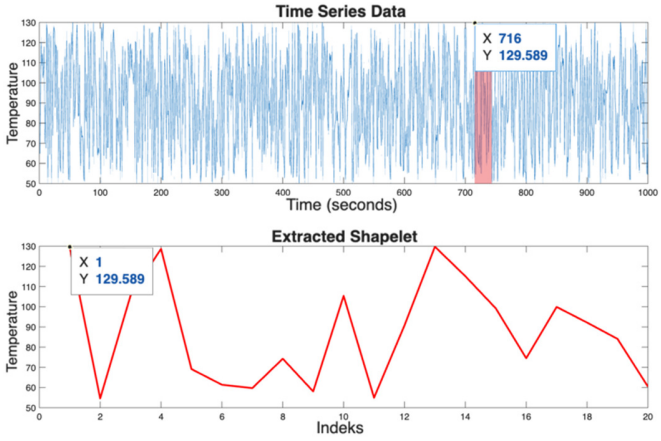

Fig. 6. Temperature time series and extracted shapelet.

The top plot in Figure 6 shows the time series of temperature measurements. The x-axis indicates time (in seconds), and the y-axis shows temperature values. The bottom plot presents an extracted shapelet, a distinctive pattern or subsequence within the time series data that can be used for classification or anomaly detection. The x-axis of the bottom plot shows the shapelet index, and the y-axis displays the corresponding temperature values.

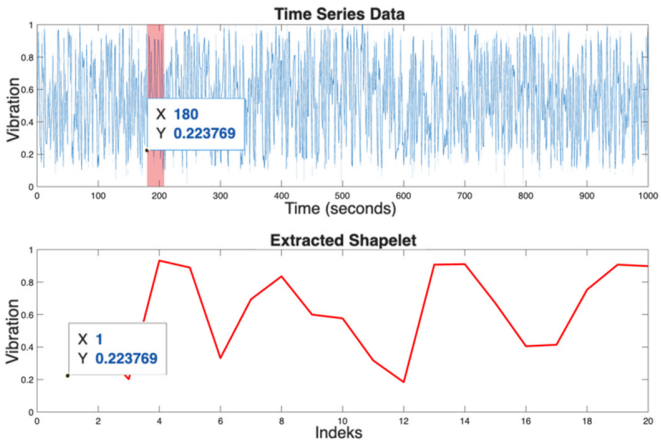

Fig. 7. Vibration time series and extracted shapelet.

The top plot in Figure 7 shows a univariate time series of vibration measurements. The x-axis represents time (in seconds), and the y-axis shows vibration values. The shapelet is extracted starting at index 1, with a vibration value of 4.223769. This shapelet offers valuable information for classifying and detecting anomalies in the IoT system, as it represents a unique and significant pattern within the vibration time series data.

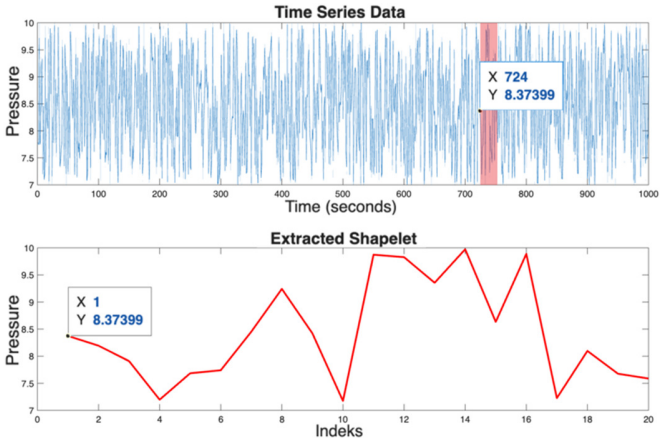

Fig. 8. Pressure time series and extracted shapelet.

The top plot in Figure 8 shows the time series of a univariate pressure measurement. The x-axis represents time (in seconds), and the y-axis shows pressure values. The bottom plot highlights an extracted shapelet from the time series data. The shapelet is extracted at index 1, with a pressure value of 8.37399. As already stated, this shapelet offers valuable information for classifying and detecting anomalies in the IoT system.

D. Comparison with Baseline Models

A comparative analysis was performed to evaluate the performance of the proposed shapelet transformation approach relative to several baseline models commonly used for time-series classification and anomaly detection in IoT systems. The objective was to assess the relative merits of the proposed method and its potential to surpass established techniques. The baseline models comprised SVM, a supervised learning algorithm effective in high-dimensional spaces; Random Forest, an ensemble method that aggregates multiple decision trees to improve robustness and classification accuracy; XGBoost, a gradient boosting algorithm known for strong performance across diverse classification tasks; and Naive Bayes, a probabilistic classifier that assumes feature independence.

All baseline models were evaluated using identical datasets, feature representations, preprocessing procedures, data splits, and evaluation metrics as the proposed approach to ensure a fair and comprehensive comparison. Baseline classifiers were trained on global statistical features extracted from each sensor channel. Random Forest was configured with n_estimators = 100 and max_depth = 10; SVM utilized an RBF kernel with C = 1.0 and γ = 0.1; and XGBoost was implemented with

n_estimators = 200 and learning_rate = 0.1. For the proposed method, the same classifiers and hyperparameter settings were applied to shapelet-distance features, ensuring that any observed performance differences could be attributed solely to the shapelet-based transformation. The results of this comparative analysis are presented in this section, highlighting the advantages of the proposed method for anomaly detection in multivariate time series data.

As shown in Figure 9, all models improve in performance as the amount of training data increases from 10% to 50%, indicating the benefit of additional training examples in enhancing model generalization. Among the baseline models, XGBoost and Random Forest consistently outperform SVM and Naive Bayes at all training data levels, reflecting the advantages of ensemble and gradient boosting techniques in capturing complex patterns. The proposed shapelet-based method achieves the highest performance across all training sizes, with the performance gap widening as more data are used. This suggests that the shapelet-based approach more effectively leverages additional data by identifying discriminative short-term patterns within the multivariate time series, resulting in superior anomaly detection performance in industrial IoT datasets. These results underscore the method's ability to capture subtle temporal variations that conventional classifiers may overlook.

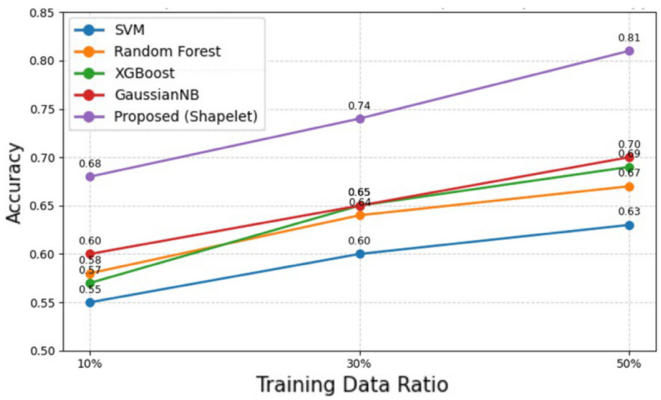

Fig. 9. Performance comparison of baseline models and the proposed shapelet-based approach across different training set sizes.

Figure 10 illustrates the performance of each baseline model in correctly and incorrectly classifying the input data. The rows correspond to the actual classes, whereas the columns represent the predicted classes. The diagonal elements show the number of correctly classified instances, and the off-diagonal elements indicate misclassified instances. Examination of the confusion matrices reveals the relative strengths and weaknesses of each model. For example, SVM and Naive Bayes models achieve a higher number of correctly classified instances (179) for certain classes, whereas Random Forest and XGBoost demonstrate a more balanced distribution between correct and incorrect classifications across all classes. Overall, these results emphasize the robustness of the shapelet-based approach in achieving consistent and accurate anomaly detection in complex multivariate time-series data.

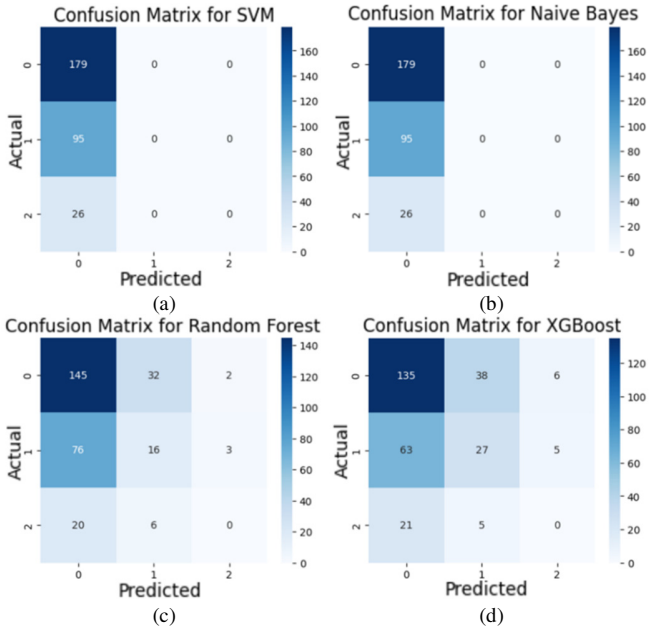

Fig. 10. Confusion matrices of baseline models: (a) SVM, (b) Naive Bayes, (c) Random Forest, (d) XGBoost.

IV. CONCLUSION

This study introduces a novel shapelet transformation approach for classifying multivariate time series data to detect anomalies in Internet of Things (IoT) systems, addressing a critical need in the evolving landscape of IoT applications, where timely and accurate anomaly detection is essential for operational efficiency and security. Rigorous experiments on multiple real-world datasets demonstrate that the proposed methodology significantly improves anomaly detection accuracy and enhances interpretability by leveraging the distinctive properties of shapelets, which capture the most informative patterns within the data.

Empirical results show that the shapelet transformation approach achieves strong performance across multiple evaluation metrics, including accuracy, precision, recall, F1-score, and the Area Under the Receiver Operating Characteristic (ROC) Curve (AUC), consistently surpassing traditional statistical methods and baseline machine learning models without shapelet-based feature extraction. These findings underscore the approach's effectiveness in accurately identifying both normal and anomalous instances, providing a robust framework for real-time monitoring across diverse IoT applications such as smart homes, industrial automation, and environmental monitoring. The ability to identify specific temporal patterns associated with anomalies supports improved decision-making by system operators and enables more targeted interventions, thereby enhancing the resilience and reliability of IoT infrastructures.

However, the study has limitations, including variability in performance across datasets and challenges related to noise and data quality. Future research should focus on optimizing shapelet extraction techniques, integrating advanced noise-

reduction strategies, and evaluating the scalability of the approach for larger datasets and real-time processing.

In summary, these findings contribute to the expanding body of knowledge in IoT anomaly detection, establishing a foundation for future advancements and applications of shapelet-based methodologies. By addressing key challenges in multivariate time series classification, this research supports the development of more effective and interpretable anomaly detection solutions, enhancing the operational integrity and security of IoT systems and promoting greater trust and reliability in IoT technology deployment across multiple domains.

ACKNOWLEDGMENT

This work was supported in part by Indonesian Education Scholarship [Beasiswa Pendidikan Indonesia (BPI)], in part by the Center for Higher Education Funding and Assessment [Pusat Pendanaan dan Asesmen Pendidikan Tinggi (PPAPT)], and in part by Indonesian Endowment Fund for Education [Lembaga Pengelola Dana Pendidikan (LPDP)].

REFERENCES

[1] M. Altin and A. Cakir, "Exploring the Influence of Dimensionality Reduction on Anomaly Detection Performance in Multivariate Time Series," *IEEE Access*, vol. 12, pp. 85783–85794, 2024, https://doi.org/10.1109/ACCESS.2024.3415088.

[2] F. Li, A. Shinde, Y. Shi, J. Ye, X.-Y. Li, and W. Song, "System Statistics Learning-Based IoT Security: Feasibility and Suitability," *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 6396–6403, Aug. 2019, https://doi.org/10.1109/JIOT.2019.2897063.

[3] I. Ullah and Q. H. Mahmoud, "Design and Development of a Deep Learning-Based Model for Anomaly Detection in IoT Networks," *IEEE Access*, vol. 9, pp. 103906–103926, 2021, https://doi.org/10.1109/ACCESS.2021.3094024.

[4] N. Imtiaz *et al.*, "A Deep Learning-Based Approach for the Detection of Various Internet of Things Intrusion Attacks Through Optical Networks," *Photonics*, vol. 12, no. 1, Jan. 2025, Art. no. 35, https://doi.org/10.3390/photonics12010035.

[5] M. Steiger *et al.*, "Visual Analysis of Time-Series Similarities for Anomaly Detection in Sensor Networks," *Computer Graphics Forum*, vol. 33, no. 3, pp. 401–410, 2014, https://doi.org/10.1111/cgf.12396.

[6] P. Biswas and T. Samanta, "A Method for Fault Detection in Wireless Sensor Network Based on Pearson's Correlation Coefficient and Support Vector Machine Classification," *Wireless Personal Communications*, vol. 123, no. 3, pp. 2649–2664, Apr. 2022, https://doi.org/10.1007/s11277-021-09257-7.

[7] N. Zhang and S. Sun, "Multiview Unsupervised Shapelet Learning for Multivariate Time Series Clustering," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 45, no. 4, pp. 4981–4996, Apr. 2023, https://doi.org/10.1109/TPAMI.2022.3198411.

[8] M. Hu *et al.*, "Detecting Anomalies in Time Series Data via a Meta-Feature Based Approach," *IEEE Access*, vol. 6, pp. 27760–27776, 2018, https://doi.org/10.1109/ACCESS.2018.2840086.

[9] A. A. A. Mohammed, "Improving Intrusion Detection Systems by Using Deep Learning Methods on Time Series Data," *Engineering, Technology & Applied Science Research*, vol. 15, no. 1, pp. 19267–19272, Feb. 2025, https://doi.org/10.48084/etasr.9417.

[10] F. Wang, Y. Jiang, R. Zhang, A. Wei, J. Xie, and X. Pang, "A Survey of Deep Anomaly Detection in Multivariate Time Series: Taxonomy, Applications, and Directions," *Sensors*, vol. 25, no. 1, Jan. 2025, Art. no. 190, https://doi.org/10.3390/s25010190.

[11] H.-S. Huang, C.-L. Liu, and V. S. Tseng, "Multivariate Time Series Early Classification Using Multi-Domain Deep Neural Network," in *2018 IEEE 5th International Conference on Data Science and Advanced Analytics*, Turin, Italy, 2018, pp. 90–98, https://doi.org/10.1109/DSAA.2018.00019.

[12] H. Darvishi, D. Ciuonzo, and P. S. Rossi, "Real-Time Sensor Fault Detection, Isolation and Accommodation for Industrial Digital Twins," in *2021 IEEE International Conference on Networking, Sensing and Control*, Xiamen, China, 2021, pp. 1–6, https://doi.org/10.1109/ICNSC52481.2021.9702175.

[13] A. Alrefaei and M. Ilyas, "Using Machine Learning Multiclass Classification Technique to Detect IoT Attacks in Real Time," *Sensors*, vol. 24, no. 14, July 2024, Art. no. 4516, https://doi.org/10.3390/s24144516.

[14] A. Bagnall, J. Lines, J. Hills, and A. Bostrom, "Time-Series Classification with COTE: The Collective of Transformation-Based Ensembles," *IEEE Transactions on Knowledge and Data Engineering*, vol. 27, no. 9, pp. 2522–2535, Sept. 2015, https://doi.org/10.1109/TKDE.2015.2416723.

[15] F. J. Baldán and J. M. Benítez, "Multivariate times series classification through an interpretable representation," *Information Sciences*, vol. 569, pp. 596–614, Aug. 2021, https://doi.org/10.1016/j.ins.2021.05.024.

AUTHORS PROFILE

Wahyuddin S. was born in Malaka-Bone, South Sulawesi, in 1992. He completed his undergraduate studies at Dipa Makassar University (UNDIPA) in 2015. He earned a Master's degree in Information Systems from Indonesia Computer University (UNIKOM), Bandung, in April 2019. In 2023, he began doctoral studies in the Computer Science program at Sepuluh Nopember Institute of Technology (ITS) Surabaya.

Ahmad Saikhu (Member, IEEE) received the bachelor's degree from the Statistics Department, Institut Teknologi Sepuluh Nopember (ITS), Indonesia, in 1994, the M.T. degree from the Informatics Department, ITS, in 2000, and the Ph.D. degree from the Computer Science Department, ITS, in 2019. He has been a Lecturer with the Informatics Department, ITS, since 2006. He actively engages in informatics research and serves as a reviewer for several journals and conferences. His primary research interests include data mining and time series.

Agus Budi Raharjo received the Ph.D. degree from Aix-Marseille University, France, in 2020. He is currently an Assistant Professor with the Institut Teknologi Sepuluh Nopember, Surabaya. He has published over 35 international publications and conference papers. His research interests include machine learning, cloud computing, telemedicine, and data science.