iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** VIII **Month of publication:** Aug 2023

DOI: https://doi.org/10.22214/ijraset.2023.55226

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue VIII Aug 2023- Available at www.ijraset.com

Study of Anomaly Detection in IoT Sensors

Jewan Jot[1], Prof. Lalit Sen Sharma[2]
Department of CS&IT, University of Jammu

Abstract: ***The rapid proliferation of Internet of Things (IoT) technology has resulted in an exponential increase in the number of connected devices and sensors. These sensors play a crucial role in collecting and transmitting data, enabling various applications and services in diverse domains. However, the large-scale deployment of IoT sensors also introduces new challenges, particularly in the realm of anomaly detection. This research paper presents a comprehensive study of anomaly detection techniques specifically designed for IoT sensors. We delve into the different types of anomalies that can occur in IoT sensor data, including sudden changes, outliers, and malicious attacks. Moreover, we explore the unique characteristics and requirements of IoT sensor networks, such as resource constraints, heterogeneous data, and dynamic network topologies. To address these challenges, we provide an overview of state-of-the-art anomaly detection methods tailored to IoT sensor networks. These methods encompass both traditional statistical approaches and machine learning algorithms, considering their applicability and effectiveness in the IoT context. We discuss the strengths and limitations of each technique, highlighting their suitability for different anomaly detection scenarios. Furthermore, we analyze and compare the performance of these methods using real-world IoT sensor datasets, evaluating their accuracy, efficiency, and scalability. The findings of our study shed light on the strengths and limitations of existing techniques, enabling researchers and practitioners to make informed decisions when choosing an appropriate anomaly detection method for their IoT sensor networks. By enhancing the reliability and security of IoT sensor networks, the outcomes of this research contribute to the advancement of IoT technology and its widespread adoption in various domains, including smart cities, healthcare, transportation, and industrial automation.***

Keywords: Internet of Things (IoT), anomaly detection, sensors, KNN, resource constraints, heterogeneous data, dynamic network topology, machine learning algorithms, effectiveness, accuracy, reliability, security.

I. INTRODUCTION

The Internet of Things (IoT) has revolutionized how we interact with technology and the world around us. It is a network of interconnected devices, sensors, and objects that can communicate with each other and exchange data without human intervention. This technology has gained significant attention and has become a driving force behind digital transformation across various sectors [1].

IoT sensors, in particular, play a pivotal role in the IoT ecosystem. These sensors are deployed in a wide range of applications and environments to monitor and capture data from the physical world. They are responsible for collecting information such as temperature, humidity, pressure, light, motion, and various other parameters, depending on the specific context.

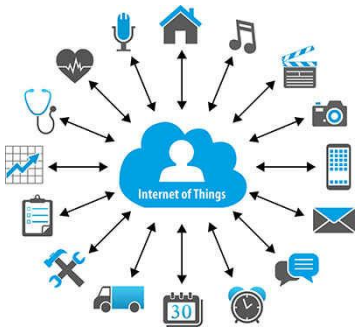


Fig.1. IOT Devices

The proliferation of IoT sensors has resulted in an exponential growth in the volume of data generated. These sensors continuously gather data from their surroundings, creating massive streams of information. This wealth of data holds immense potential for deriving insights, optimizing processes, and making informed decisions [2].

However, the sheer scale and complexity of IoT sensor data present significant challenges. One of the key challenges is the detection of anomalies within this data. Anomalies refer to observations that deviate significantly from the expected patterns or behaviors. These anomalies can arise due to various factors, including equipment malfunctions, environmental changes, human errors, and even malicious activities [2].

Accurate and timely anomaly detection in IoT sensor data is crucial for several reasons. Firstly, it enables the early identification of abnormal behavior or events, allowing for proactive measures to be taken. For instance, in an industrial setting, the detection of an anomaly in a machine's performance can help prevent costly breakdowns and downtime. In healthcare, anomaly detection in vital signs monitoring can alert healthcare professionals to potential health risks and trigger timely interventions [3].

Secondly, anomaly detection plays a crucial role in ensuring the reliability and security of IoT sensor networks. Anomalies can be indicative of potential cybersecurity threats, such as intrusion attempts or data breaches. By promptly detecting and responding to these anomalies, organizations can mitigate risks and safeguard their systems and data.

Given the critical importance of anomaly detection in IoT sensor data, there is a need for comprehensive research and analysis of the various techniques and approaches available. This paper aims to address this need by conducting a thorough study of anomaly detection techniques specifically designed for IoT sensors. By examining the different types of anomalies in IoT sensor data and providing an overview of state-of-the-art anomaly detection methods [4].

II. PROBLEM STATEMENT

The widespread adoption of Internet of Things (IoT) technology has led to exponential growth in the number of connected devices and sensors. IoT sensors play a vital role in collecting and transmitting data, enabling various applications and services. However, the large-scale deployment of IoT sensors also introduces new challenges, particularly in anomaly detection. Anomalies in IoT sensor data can occur due to a variety of reasons, including sensor malfunctions, environmental changes, cyber-attacks, or even human errors. Detecting and identifying these anomalies is crucial for maintaining the reliability, security, and efficiency of IoT sensor networks [5].

Therefore, the problem addressed in this research is to identify anomalies in IoT sensors using various techniques, including statistical techniques, cluster-based techniques, and nearest-neighbor techniques. These techniques offer different approaches and algorithms to detect anomalies in IoT sensor data.

III.TYPES OF ANOMALIES

Anomalies in IoT sensor data refer to patterns or events that deviate from the expected or normal behavior. These anomalies can arise due to various factors, including sensor malfunctions, environmental changes, security breaches, or critical events. Understanding the different types of anomalies that can occur in IoT sensor data is crucial for developing effective anomaly detection techniques. Here, we discuss some of the commonly observed types of anomalies:

A. Point Anomalies

Point anomalies, also known as global anomalies, are individual data points that significantly differ from the overall distribution of the sensor data. These anomalies can occur due to sensor faults, measurement errors, or sudden and unusual events. Point anomalies can be detected by analyzing the statistical properties of the sensor readings, such as mean, standard deviation, or distance from the normal data cluster.

B. Contextual Anomalies

Contextual anomalies occur when a specific sensor reading deviates from the expected behavior based on its contextual information. In IoT sensor networks, sensors often capture data that is interrelated or dependent on other sensors or contextual factors. Detecting contextual anomalies involves analyzing the relationships and dependencies between multiple sensor readings to identify inconsistencies or abnormal patterns.

C. Collective Anomalies

Collective anomalies, also known as contextual anomalies, are patterns of sensor readings that exhibit abnormal behavior when considered collectively. These anomalies are challenging to detect because individual sensor readings may appear normal, but their collective behavior or correlation may deviate significantly from the expected behavior. Detecting collective anomalies requires analyzing the interrelationships and dependencies among multiple sensors or groups of sensors.

D. Temporal Anomalies

Temporal anomalies refer to abnormal patterns or events that occur over time in IoT sensor data. These anomalies can involve sudden changes, trends, periodicity, or seasonality in the sensor readings. Detecting temporal anomalies requires analyzing the time series characteristics of the sensor data, such as trend analysis, seasonal decomposition, or change point detection algorithms.

E. Spatial anomalies

Spatial anomalies occur when the geographical or spatial distribution of sensor readings deviates from the expected patterns. In IoT sensor networks deployed in large-scale environments, spatial anomalies can indicate localized abnormalities, sensor failures, or environmental variations. Detecting spatial anomalies involves analyzing spatial relationships, clustering techniques, or spatial statistics to identify regions with abnormal sensor readings. Understanding these different types of anomalies in IoT sensor data is crucial for developing effective anomaly detection techniques. Each type of anomaly requires specific analysis techniques and algorithms tailored to the characteristics of the sensor data and the underlying IoT network. By identifying and categorizing these anomalies, researchers and practitioners can develop targeted approaches to detect and mitigate abnormal behavior in IoT sensor networks, improving their reliability, efficiency, and security [6] [7] [8] [9].

IV. METHODOLOGY

The research paper adopts a combination of statistical analysis, cluster-based techniques, and nearest-neighbor techniques for anomaly detection in IoT sensor data collected using Raspberry Pi.

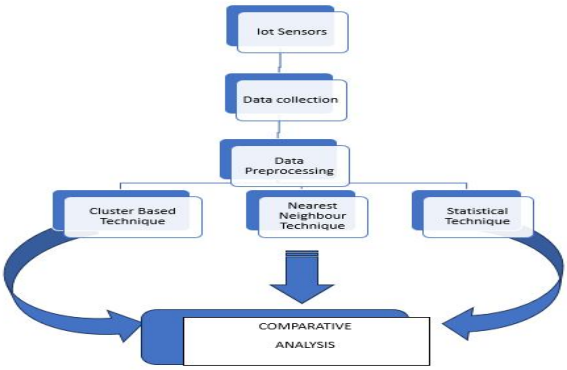


Fig:2. Methodology

The methodology includes data collection using specific IoT sensors, setting up Raspberry Pi, sensor wiring and configuration, library installation, and data collection script development. For statistical analysis, the Z-Score method is utilized, providing promising results with high precision and moderate recall. The K-Means algorithm is applied for cluster-based techniques, showing good precision and high recall, making it a preferred method for certain sensors. The Nearest Neighbor Technique (KNN) exhibits varying performance with moderate overall F1 scores, suggesting further fine-tuning and feature engineering may be required. The paper emphasizes the importance of considering class distribution, and real-world consequences of false positives and negatives, and encourages further research to improve the anomaly detection process for each sensor's context. Additionally, the study highlights the application of K-means clustering and KNN algorithms in detecting various types of anomalies in time series data, depending on data characteristics and specific anomaly requirements. However, it stresses the need to combine multiple approaches and utilize domain knowledge for accurate anomaly detection [8]. In this research study, the anomaly detection techniques were specifically applied and tested on data collected from four distinct sensors: the temperature and humidity sensor, ultrasonic distance sensor, LDR sensor, and soil moisture sensor. These sensors were selected based on their relevance to the IoT application under investigation, as they provide crucial environmental and contextual data. The primary objective was to assess the performance of different anomaly detection methods for each of these sensors individually [9]. By focusing solely on these four sensors, the research aimed to gain valuable insights into the effectiveness of statistical analysis with Z-Scores, cluster-based techniques with K-Means, and nearest neighbor techniques with KNN for detecting anomalies in diverse types of sensor data. The choice of these sensors allowed for a comprehensive examination of anomaly detection across various environmental factors, making the findings applicable to a wide range of IoT scenarios.

A. Statistical Technique

Statistical techniques, particularly the Z-Score method, are widely used for anomaly detection in IoT sensor data. The Z-Score technique calculates the standard deviation of a sensor data attribute and identifies data points that deviate significantly from the mean as anomalies.

Z-scores provide a standardized measure to compare data points across different datasets or variables with varying scales. They find applications in outlier detection, data normalization, and hypothesis testing [10]. The methodology for statistical anomaly detection involves modeling the normal behavior of the data and identifying instances that deviate significantly from the expected patterns. Common types of anomalies detected using statistical techniques include point anomalies, contextual anomalies, trend anomalies, seasonal anomalies, and residual anomalies.

Combining multiple statistical techniques and leveraging domain knowledge can enhance the accuracy of anomaly detection in time series data. Overall, statistical techniques play a crucial role in early anomaly detection, improving the reliability and performance of IoT systems.

B. Cluster-Based Technique

Cluster-Based Techniques, specifically K-Means Clustering, are unsupervised learning algorithms used for grouping unlabeled datasets into different clusters based on similarity. The algorithm aims to minimize the sum of distances between data points and their corresponding cluster centroids.

The process involves selecting the number of clusters (K), assigning data points to their closest centroids, and iteratively updating centroids until convergence is reached.

In this research paper's methodology, cluster-based techniques were applied to the IoT sensor data, focusing on the four sensors: temperature and humidity, ultrasonic distance, LDR, and soil moisture sensors.

The goal was to identify anomalies by detecting data points dissimilar to any cluster or exhibiting significant deviations from their assigned cluster centroids.

While K-means clustering is primarily designed for grouping data into clusters, it can be utilized for anomaly detection in time series data.

Anomalies can be identified as cluster-based anomalies, shape-based anomalies, outliers, or deviations from cluster behavior. However, the effectiveness of K-means for anomaly detection depends on the data's characteristics and the specific types of anomalies being targeted.

Overall, the research highlights the potential of K-means clustering as a cluster-based technique for anomaly detection in IoT sensor data. It also emphasizes the importance of combining multiple approaches and domain knowledge to enhance anomaly detection accuracy and reliability in diverse time series data.

C. Nearest Neighbour Technique

In summary, the K-Nearest Neighbor (KNN) algorithm is a simple supervised learning technique used for classification and regression tasks.

It classifies a new data point by finding the k most similar data points in the training set and assigning the new data point to the category that is most prevalent among its k-nearest neighbors is a non-parametric and lazy learner algorithm, meaning it does not make assumptions about the underlying data and stores the entire training dataset for classification at the time of prediction. It can be used for both classification and regression, but it is mostly applied to classification problems.

While KNN is not specifically designed for anomaly detection, it can be adapted for this purpose in time series data. The methodology involves selecting the number of neighbors (k) and calculating the distance between data points to identify anomalies based on their dissimilarity to their nearest neighbors.

The types of anomalies that can be detected with KNN on time series data include distance-based anomalies, nearest neighbor outliers, temporal contextual anomalies, and local outliers. However, the choice of k value and distance metric can significantly impact the accuracy of anomaly detection. Incorporating domain knowledge and considering the specific characteristics of the time series data are essential for effectively detecting anomalies.

Overall, while KNN can be used for anomaly detection in time series data, it is often beneficial to combine it with other specialized techniques designed explicitly for time series anomaly detection to achieve better performance and coverage [1].

V. ANALYSIS OF RESULTS

A. *Results of Anomaly Detection Through Statistical Analysis* Using Z-Scores:

TABLE I
RESULTS

Evaluation Metrics for Anomaly Detection through Statistical Analysis using Z-Scores				
Results	Temperature and Humidity Sensor (Dht11)	LDR sensor	Ultrasonic Distance Sensor	Soil Moisture Sensor
Precision	1.0	0.75	1.0	0.18
Recall	0.5	1.0	0.54	1.0
F1	0.6666	0.857	0.705	0.307
Accuracy	0.98	0.99	0.95	0.955

Results of Anomaly Detection Through Cluster-Based Technique Using K-Means:

TABLE II
RESULTS

Evaluation Metrics for Anomaly Detection Through Cluster-Based Technique Using K-Means				
Results	Temperature and Humidity Sensor (Dht11)	LDR sensor	Ultrasonic Distance Sensor	Soil Moisture Sensor
Precision	1.0	0.6	0.4	0.33
Recall	0.75	1.0	0.181	1.0
F1	0.85	0.749	0.25	0.5
Accuracy	0.99	0.98	0.88	0.98

Results of Anomaly Detection Through Nearest Neighbor Technique using K- Nearest Neighbor

TABLE III
RESULTS

Evaluation Metrics for Anomaly Detection through Nearest Neighbor Technique Analysis using KNN				
Results	Temperature and Humidity Sensor (Dht11)	LDR sensor	Ultrasonic Distance Sensor	Soil moisture Sensor
Precision	1.0	0.6	1.0	0.25
Recall	0.75	1.0	0.4545	1.0
F1	0.85	0.749	0.625	0.4
Accuracy	0.99	0.98	0.94	0.97

Anomaly detection is a critical task in various fields to identify rare and abnormal instances that deviate from the norm. Three different techniques for anomaly detection were evaluated: statistical analysis using Z-scores, cluster-based technique using K-means, and nearest neighbor technique using KNN. Each technique was applied to four different sensor datasets, and their performance was evaluated using precision, recall, F1 score, and accuracy metrics.

Statistical analysis using Z-scores showed high precision for the Temperature and Humidity Sensor data and the Ultrasonic Distance Sensor, indicating that the majority of detected anomalies were true anomalies. However, the recall was relatively lower for these sensors, indicating that some actual anomalies were missed. The LDR Sensor had reasonably good precision and recall, while the Soil Moisture Sensor had the lowest precision, capturing only a small proportion of actual anomalies. Overall, accuracy was high but might be affected by class imbalance.

The cluster-based technique using K-means achieved high precision for the Temperature and Humidity Sensor (Dht11) and the Ultrasonic Distance Sensor, but moderate precision for the LDR Sensor and low precision for the Soil Moisture Sensor. The recall was high for the LDR Sensor and the Soil Moisture Sensor, but lower for the other two sensors. The F1 score was highest for the Temperature and Humidity Sensor, followed by the LDR Sensor. Accuracy was generally high but might not fully reflect true anomaly detection performance.

The nearest neighbor technique using KNN achieved high precision for the Temperature and Humidity Sensor and the Ultrasonic Distance Sensor, moderate precision for the LDR Sensor, and low precision for the Soil Moisture Sensor. The recall was high for the LDR Sensor and the Soil Moisture Sensor, but lower for the other two sensors. The F1 score was highest for the Temperature and Humidity Sensor (, followed by the LDR Sensor. Accuracy was generally high, but like the other techniques, it might not fully capture the performance in imbalanced datasets.

VI. DISCUSSION OF FINDINGS

Anomaly detection techniques, namely Statistical Analysis with Z-Scores, Cluster-Based Technique with K-Means, and Nearest Neighbor Technique with KNN were evaluated on four sensors: Temperature and Humidity Sensor (Dht11), LDR Sensor, Ultrasonic Distance Sensor, and Soil Moisture Sensor. The results were analyzed using precision, recall, F1 score, and accuracy metrics.

Statistical Analysis with Z-Scores demonstrated high precision, accurately identifying true anomalies, but had moderate recall, missing some anomalies. Cluster-Based Technique with K-Means showed good precision for most sensors, except for LDR and Soil Moisture Sensors, and had high recall, effectively capturing actual anomalies within clusters. The nearest Neighbor Technique with KNN had variable precision and recall across sensors, with good performance for LDR and Soil Moisture Sensors.

The F1 score, representing the balance between precision and recall, was reasonable for Z-Scores but varied for K-Means and KNN. Accuracy was high for all techniques, indicating the successful classification of instances.

Each technique has strengths and weaknesses, and the choice should align with domain-specific requirements and the trade-off between false positives and false negatives. Further optimization may be needed for certain sensors.

The evaluation highlights the effectiveness of K-Means for most sensors and suggests potential improvements for KNN and Z-Scores methods. The findings underscore the importance of considering data characteristics and application-specific needs when selecting an anomaly detection technique for each sensor.

VII. COMPARISON OF TECHNIQUES AND THEIR ADVANTAGES/DISADVANTAGES

When comparing the different anomaly detection techniques, it is essential to consider their advantages and disadvantages. Here's a comparison of the techniques discussed, along with their respective Advantages and disadvantages.

A. Statistical Analysis using Z-Scores

1) Advantages

- High precision and accuracy for anomaly detection.
- Relatively simple and straightforward implementation.
- Effective in identifying anomalies based on statistical deviations.

2) Disadvantages

- Lower recall compared to other techniques, indicating the possibility of missing some anomalies.
- Reliance on assumptions of normality and data distribution, which may limit its applicability to certain datasets.
- Lack of adaptability to dynamic or changing data patterns.

B. Cluster-Based Technique using K-Means

1) Advantages:

- Ability to identify clusters and detect anomalies based on their deviation from the clusters.
- Relatively simple and scalable algorithm.
- Potential for detecting complex anomalies within clusters.

2) Disadvantages

- Sensitivity to the initial cluster centroids, which may result in suboptimal solutions.
- Difficulty in determining the appropriate number of clusters (K).
- Limited ability to handle overlapping or non-linearly separable data.

C. Nearest Neighbor Technique using KNN

1) Advantages

- Ability to capture local patterns and detect anomalies based on the similarity to neighboring instances.
- Flexibility to adjust the K value to control the balance between precision and recall.
- Suitable for handling high-dimensional data and nonlinear relationships.

2) Disadvantages

- Computationally expensive for large datasets, as it requires calculating distances between instances.
- Sensitivity to the choice of a distance metric, which may affect the performance.
- Reliance on the assumption that the majority of instances are normal, which may limit its effectiveness for datasets with a high proportion of anomalies.

Overall, each technique has its own strengths and weaknesses, and the choice depends on the specific requirements and characteristics of the dataset. The statistical analysis using Z-scores is effective for detecting anomalies based on statistical deviations, while the cluster-based technique using K-means leverages clustering to identify deviations from normal patterns. The nearest neighbor technique using KNN focuses on local patterns and similarities to detect anomalies. Consider the nature of the data, the desired balance between precision and recall, computational efficiency, and the ability to handle different data distributions when selecting the appropriate technique for anomaly detection.

VIII. PRACTICAL IMPLICATIONS AND RECOMMENDATIONS

The findings and comparison of anomaly detection techniques have practical implications and recommendations for real-world applications. To enhance anomaly detection effectiveness, practitioners should consider the nature of the data, trade-offs between precision and recall, and evaluate performance metrics holistically using the F1 score. They should also assess computational efficiency for large-scale datasets, incorporate domain knowledge, and explore ensemble or hybrid approaches for robust results. Continuous monitoring and periodic evaluation are vital for adapting to data changes, and staying updated with the latest research enables leveraging emerging techniques. By following these recommendations, practitioners can make informed decisions, improve anomaly detection accuracy, and ensure effective anomaly detection systems in real-world scenarios.

Anomaly detection is an active research area, and ongoing advancements and new techniques are being developed. Stay updated with the latest research and explore emerging methods that may offer improved performance or address specific challenges in anomaly detection for your application domain.

By considering these practical implications and recommendations, you can make informed decisions when selecting and implementing anomaly detection techniques and enhance the effectiveness and reliability of your anomaly detection system.

A. Limitations of the Study

The comparative analysis of anomaly detection techniques has several limitations that should be acknowledged. Firstly, the study's findings are based on a specific dataset, and the performance of the techniques may vary when applied to different datasets with diverse characteristics. Secondly, while the study used multiple evaluation metrics, other metrics not considered in the study could provide additional insights into the techniques' performance. Thirdly, the study focused on a limited set of techniques, excluding advanced approaches, potentially missing out on other effective methods. Fourthly, optimal parameter tuning for each technique was not extensively explored, which could affect their performance. Additionally, the study's controlled experimental setting may not fully reflect real-world deployment challenges and factors that could influence technique performance. The study did not explicitly address feature engineering, and the quality of features used could impact the results. Lastly, using a single evaluation dataset may limit the generalizability of the findings, and a more extensive evaluation with diverse datasets would enhance the study's robustness.

B. Future Research Directions

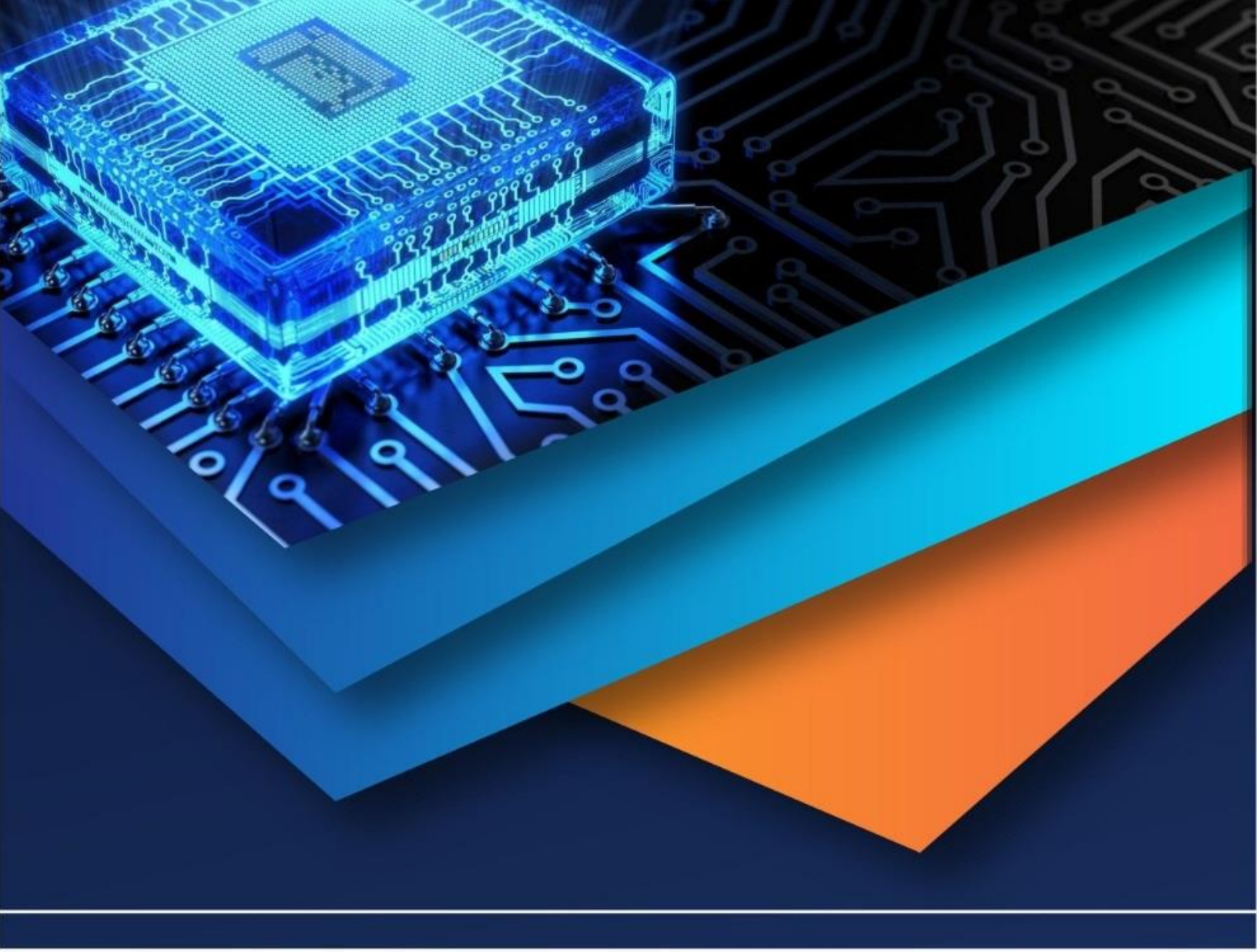
The comparative analysis of anomaly detection techniques has paved the way for several promising avenues of future research. Firstly, exploring advanced anomaly detection techniques like deep learning-based models and graph-based methods holds the potential for improving accuracy, scalability, and applicability to diverse data types. Secondly, investigating ensemble approaches that combine multiple techniques could lead to enhanced anomaly detection performance. Unsupervised and semi-supervised techniques offer opportunities to handle scarce labeled data and adapt to evolving data environments. Additionally, developing explainable anomaly detection methods would enhance user trust and understanding. Online anomaly detection for dynamic data streams and establishing benchmark datasets and evaluation protocols are essential for objective comparisons. Incorporating domain knowledge and conducting real-world application studies will further validate the practical effectiveness of these techniques in specific domains. By addressing these research directions, the field of anomaly detection can advance and provide valuable insights for various industries and applications.

IX. CONCLUSION

In conclusion, the anomaly detection study utilizing Statistical Analysis with Z-Scores, Cluster-Based Technique with K-Means, and Nearest Neighbor Technique with KNN for different sensors (Temperature and Humidity Sensor, LDR Sensor, Ultrasonic Distance Sensor, and Soil Moisture Sensor) reveals valuable insights. Z-Scores demonstrate high precision, moderate recall, and reasonable F1 scores, while K-Means exhibit good precision, high recall, and balanced F1 scores, making it a preferred choice for some sensors. KNN shows varying performance, needing further fine-tuning and feature engineering. Selecting the appropriate technique depends on specific requirements and trade-offs. Considering class distribution and real-world consequences of false positives and negatives is essential, and further research is encouraged to enhance the anomaly detection process for each sensor's context.

REFERENCES

[1] A. Gaddam, T. Wilkin and M. Angelova, "Anomaly Detection Models for Detecting Sensor Faults and Outliers in the IoT - A Survey," 2019 13th International Conference on Sensing Technology (ICST), 2019, pp. 1-6.
[2] D. Sehrawat and N. S. Gill, "Smart Sensors: Analysis of Different Types of IoT Sensors," 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI), 2019, pp. 523-528.
[3] Run-Xia Guo, Kai Guo, Jian-Kang Dong, Fault diagnosis for sensors in a class of nonlinear systems, IMA Journal of Mathematical Control and Information, Volume 35, Issue 2, June 2018, Pages 375– 391
[4] Daoliang Li, Ying Wang, Jinxing Wang, Cong Wang, Yanqing Duan, Recent advances in sensor fault diagnosis: A review, Sensors, and Actuators A: Physical, Volume309,2020,111990, ISSN0924 4247
[5] Y. Hida, P. Huang, and R. Nishtala, “Aggregation query under uncertainty in sensor networks,” Department of Electrical Engineering and Computer Science. The University of California, Berkeley, Tech. Rep, 2004.
[6] S. Bharti, K. K. Pattanaik, and A. Pandey, “Contextual outlier detection for wireless sensor networks,” Journal of Ambient Intelligence and Humanized Computing, 2019.
[7] M. Ahmed, A. Naser Mahmood, and J. Hu, “A survey of network anomaly detection techniques,” 2016.
[8] I. Lee and K. Lee, “The Internet of things (IoT): Applications, investments, and challenges for enterprises,” Business Horizons, vol. 58, no. 4, pp. 431–440, 2015.
[9] Chen, M., Gonzalez, S., & Mao, S. (2014). Big data: A survey. Mobile Networks and Applications, 19(2), 171-209.
[10] Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. ACM Computing Surveys (CSUR), 41(3), 1-58.
[11] Akkaya, K., Senel, F., & Ulusar, U. D. (2019). A comprehensive survey on anomaly detection in IoT systems. Journal of Network and Computer Applications, 127, 48-67.
[12] Akkaya, K., Ulusar, U. D., & Şenel, F. (2020). A survey on machine learning techniques for anomaly detection in IoT systems. Journal of Network and Computer Applications, 150, 102508.
[13] Liu, F., Zhang, C., & Chen, C. (2018). Anomaly detection in IoT data using deep learning approaches. Future Generation Computer Systems, 87, 278-287.
[14] Pan, S., Chen, X., Zhu, X., & Long, G. (2020). Deep anomaly detection with outlier exposure. In Proceedings of the AAAI Conference on Artificial Intelligence, 34(07), 6292-6299.
[15] Ahmad, I., Lloret, J., Cano, J. C., & Macià-Pérez, F. (2020). Machine learning-based intrusion detection system for the Internet of things in edge computing environments. Sensors, 20(16), 4497.
[16] Özdemir, S., Uluagac, A. S., & Beyah, R. (2017). A survey on anomaly detection for cyber-physical systems. ACM Computing Surveys (CSUR), 50(3), 40.
[17] Papadimitriou, S., Shilton, A., Thakker, D., Lepri, B., & Kostakos, V. (2018). Anomaly detection in IoT for urban spaces: A survey. ACM Computing Surveys (CSUR), 51(2), 1-34.
[18] Li, M., Zheng, Y., Li, S., & Li, H. (2019). Deep learning for anomaly detection: A review. Neurocomputing, 335, 98-112.
[19] M. Mallick, A. Misra, N. Ganguly, and Y. Lee, "DETECTIVES: Unified Detection & Correction of IoT Faults in Smart Homes," 2020 IEEE 21st International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM), 2020, pp. 78-87.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY