Current Journal of Engineering and Science Research
Volume 2, Issue 2, pp 6-11, February 2025
ISSN (online): 3049-1738
DOI: https://doi.org/10.47001/CJESR/2025.202002
Available Online at https://www.cjesr.com

Automated Machine Learning Methods for Identification of Anomalies in IoT Sensor Networks

Swapnil Deshpande

Department of Electronic Science, Savitribai Phule Pune University, Pune, Maharashtra, India

Abstract: The identification of anomalies in intelligent IoT sensor networks (SISN) is important to recognize atypical events or behaviors that can indicate security gaps or operational challenges. Conventional methods based on predefined rules are often inappropriate due to the complex and constantly developing nature of IoT ecosystems. On the other hand, automatic learning techniques (ML) have occurred as practical alternatives, with algorithms being used that learn data in order to identify themselves independently. In this journal article, a variety of ML strategies are examined that are used to detect anomalies in SISN that covers supervised learning approaches without supervision and semi-super-supervised. It deals with critical components such as data preparation, properties and selection of suitable algorithms to improve the accuracy and efficiency of recognition. Case studies are presented to demonstrate the use of ML techniques in IoT scenarios in the real world, which shows their effectiveness in the identification of different anomalies. In addition, the article examines evaluation measures for measuring the detection performance with an approach for measures such as precision, memory and F1 score. In summary, the article provides information on existing challenges, possible research routes and the potential influence of recognizing ML -anomalies to improve safety and reliability intelligent IoT -sensor networks.

Keywords: Machine Learning, Identification of Anomalies, Sensor Networks, SISN, ML, AI, IoT ecosystems, Conventional methods.

I. INTRODUCTION

The identification of anomalies in Internet sensor networks of intelligent (IoT) (sisn) is essential to recognize atypical behavior or events that can accommodate possible operational threats or challenges. IoT systems consist of interconnected devices that collect and share extensive data, which means that they are susceptible to different anomalies, including cyber attacks, devices of devices, environmental fluctuations or unforeseen system behavior. These anomalies can deeply influence the reliability, security and performance of IoT implementations. The diagram of the IoT sensor network is shown in Figure 1.

Conventional approaches to recognize anomalies in the configuration of structured data generally depend on defined rules or thresholds, which may not be necessary for the flexibility to change the dynamic and constant nature in IoT environments. On the contrary, automatic learning methods (ML) have due to their ability to learn data independently of one another and identify anomalies without having to create explicit rules. ML models can evaluate a wide range of IoT sensor data such as temperature, air humidity, movement and environmental information in order to determine normal behavior and to recognize the indicative deviations of anomalies.

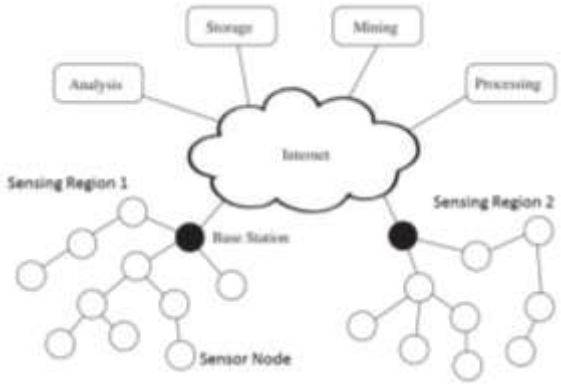

Figure 1: IoT Sensor Network Diagram

Accessed learning techniques include the training of ML models in data records, which are classified as normal or abnormal classification of data sets depending on the established models. The automatic learning workflow for the detection of anomalies in IoT is shown in Figure 2. On the contrary, indispensable learning identifies anomalies in non -sealed data by capturing models that deviate significantly from the typical behavior. The semi-super-supervised learning melts the aspects

Current Journal of Engineering and Science Research
Volume 2, Issue 2, pp 6-11, February 2025
ISSN (online): 3049-1738
DOI: https://doi.org/10.47001/CJESR/2025.202002
Available Online at https://www.cjesr.com

of the two methods with a limited amount of marked data in order to identify anomalies in larger and non-labeled data records. These ML techniques are used in different phases of detection of anomalies in the SISN that cover the pretreatment of the data, the extraction of the properties, the formation of models and the identification of real anomalies.

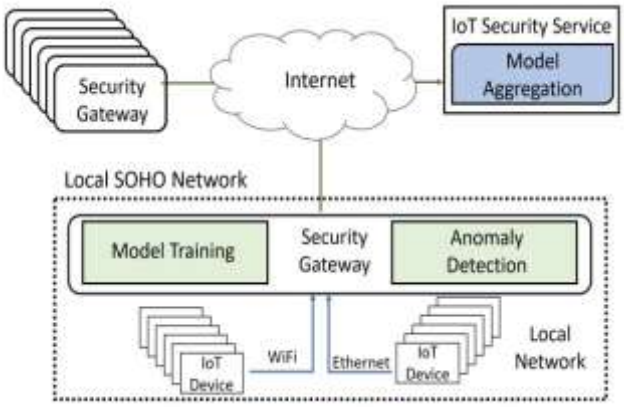

Figure 2: Machine learning workflow for anomaly detection in IoT

Return The challenges associated with the detection of anomalies in smart ioT sensor networks (SISN) implies the management of high and crazy dimension of sensor data, guarantees quick answers and overcomes the limits of IoT devices. In addition, the scalability and interpretability of automatic learning models (ML) in IoT contexts are important factors. Despite these obstacles, the anomalies, which is favored by the ML, can have significant potential to improve the security and operational efficiency of IoT implementations. Through the effective identification of possible abnormalities and threats, companies can use proactive strategies to alleviate risks, improve system reliability and to optimize the use of resources in intelligent IoT environments.

This article offers a complete general vision of detection of anomalies in intelligent IoT sensor networks and emphasizes the importance of automatic learning to meet the complexity of the IoT environments. Examine several ML techniques that are used to detect anomalies, analyze your applications in various IoT sectors and underline the need for effective data management and the model interpretability in the creation of robust anomaly recognition solutions. In the following sections, specific ML algorithms, case studies, evaluation measures and future research paths are examined in order to convey a deep understanding of the detection of anomalies in intelligent IoT sensory networks.

II. MACHINE LEARNING ALGORITHMS FOR ANOMALY DETECTION

The detection of anomalies in the Internet sensor networks is intelligent (IoT) (sisn) based on a variety of automatic learning algorithms (ML), with which sensor data models are learned and differences are to be determined compared to normal behavior. These algorithms are crucial for the improvement of the security and effectiveness of IoT implementations by automating the detection of anomalies that could mean malicious activities, system dysfunction or environmental changes [5].

Monitoring learning algorithms are effective if enough data are available. You train in data records that contain examples of normal and abnormal behavior with which you can learn models and classify new data accordingly [6]. The popular monitored methods used to detect anomalies include support vector machines (SVM) and random forests. SVM creates hyper plane to separate normal and abnormal data in high -dimensional rooms, while random forests use decision trees to classify anomalies according to the importance of the characteristic.

On the other hand, unopened learning algorithms apply in situations in which the labeled data are limited or are not available. These algorithms recognize abnormalities in data records without predefined labels by identifying data points that differ significantly from most data. Current techniques that have not been supervised to recognize anomalies include group algorithms such as K-Means and methods based on density such as DBSCAN. K-Means combines data in groups that are based on similarity and identifies atypical values as anomalies, while DBSCAN records atypical values based on differences in the data density.

Semi-Sub-oversized learning techniques combine aspects of supervised and non-monitored approaches, whereby a small amount of data is used, which are characterized for directing anomalies in larger and inconsistent data sets. This approach is particularly useful in IoT environments in which the acquisition of data marked for training can be a challenge. For example, generative enemy networks (GAN) use a generation network to create data similar to the training sentence, while a discriminatory network identifies anomalies by distinguishing real and generated data.

Automatic learning algorithms for recognizing anomalies in the SISN faces challenges such as processing of high -dimensional sensor data, adapting to dynamic environments and the operating restrictions of IoT devices. Future research is

Current Journal of Engineering and Science Research
Volume 2, Issue 2, pp 6-11, February 2025
ISSN (online): 3049-1738
DOI: https://doi.org/10.47001/CJESR/2025.202002
Available Online at https://www.cjesr.com

intended to improve scalability, resilience against the security and interpretation of the interpretation of these algorithms in order to improve their effectiveness in the IoT of the real world.

III. DATA PREPROCESSING AND FEATURE ENGINEERING FOR ANOMALY DETECTION

Receiving an effective detection of anomalies in Internet sensor networks (IoT) (SIT) (SISN) depends mainly on the pre-processing of exhaustive data and strategic functions. These preparatory steps are essential in order to optimize the performance and precision of automatic learning algorithms (ML) with which anomalies were recorded in IoT data flows [7].

The PRETEING data contain important tasks to ensure the quality and user -friendliness of the data. First of all, the unprocessed sensor data of IoT devices often contain noise, missing values or atypical values that can distort the analysis and accuracy of recognition. Techniques such as data cleaning, which include processing missing data from imputation or elimination as well as atypical detection, are used to improve data integrity. In addition, standardization or data scale helps to normalize data beaches and to reduce the effects of different amplitudes to various sensory measurements.

The properties of the properties are fundamental to the extraction of relevant ideas of unprocessed sensor data in order to admit the detection of anomalies. IoT data records generally include several attributes such as temperature, humidity, pressure and movement, which have been collected at regular intervals. The methods for selecting the properties help to identify the most important attributes that contribute to distinguishing between normal and abnormal behavior. This process reduces computer complexity and improves the effectiveness of the model by concentrating the essential models on the relevant features.

The techniques to reduce dimensionality, such as the analysis of the main components (ACP) or methods for transformation of the properties, are used to simplify high -dimensional IoT data records and at the same time maintain critical information. PCA, for example, identifies variance models in data and condenses in a smaller sentence of main components and facilitates faster calculation and better model output.

In addition, the understanding of the temporal aspects of IoT data such as trends, seasonality and periodic models is of crucial importance for the effective detection of anomalies. Chronological analysis techniques such as mobile average values, the decomposition of Fourier trends and transformations are used to capture temporary dependencies and cyclical behaviors that characterize normal and abnormal data models over time.

The challenges of data before treatment and the properties for the recognition of anomalies in the SISN include the management of data flows in real time, the guarantee of scalability in large data sets and adaptation to various data characteristics in several IoT implementations. Future research aims to develop pre-culture marketing methods and technical techniques of automated features that are adapted to the specific requirements of IoT environments, which improves the reliability and efficiency of anomaly recognition systems.

IV. CASE STUDIES AND APPLICATIONS OF MACHINE LEARNING IN IOT ANOMALY DETECTION

Automatic learning techniques (ML) have revolutionized the detection of anomalies in the Internet sensor networks of Intelligent (IOT) (SIT) (SIT), which enables proactive identification of abnormal behavior or events that could influence the integrity or performance of the system. Several case studies illustrate the practical applications and the efficiency of the ML when detecting anomalies in several IoT fields.

In industrial IoT configuration, ML algorithms are implemented in order to monitor the devices and machine output, which includes differences compared to normal operating models that may indicate impending errors or maintenance requirements [8]. For example, predictive maintenance systems use ML to analyze data from the sensor for manufacturing devices and enable an intervention in a time to prevent expensive decomposition and optimize operational efficiency.

In intelligent medical care, the recognition of ML -anomalies improves the monitoring of patients and medical care. IoT devices collect a continuous flow rate of physiological data such as heart rate, blood pressure and temperature as well as patients [9]. ML models analyze this data to identify abnormalities that can indicate health states or critical irregularities, which causes medical interventions in good time and improves the results of patients.

Environmental monitoring is another critical area in which ML plays a fundamental role. IoT sensors used in environmental monitoring networks collect data on air quality, pollution level and climatic conditions [10]. ML algorithms analyze these data flows in order to recognize unusual models or trends that can

Current Journal of Engineering and Science Research
Volume 2, Issue 2, pp 6-11, February 2025
ISSN (online): 3049-1738
DOI: https://doi.org/10.47001/CJESR/2025.202002
Available Online at https://www.cjesr.com

indicate environmental risks or abnormal changes, making quick reactions and reduction measures easier.

In addition, the detection of ML -based anomalies is an essential part of the cyber security guarantee in IoT implementations. ML models analyze the interactions for network traffic, user behavior and devices to recognize suspicious activities or intrusions that remove from normal models. By determining previous security threats, companies can carry out preventive measures to protect IoT systems from cyber attacks and data injuries.

V. EVALUATION METRICS AND PERFORMANCE ANALYSIS

The evaluation of the effectiveness of anomaly recognition algorithms in Internet sensor networks (IoT) (sisns) requires exhaustive evaluation measures and detailed performance analysis. These measures provide information about how automatic learning models (ML) work to recognize anomalies. This is important to optimize the reliability of the system and to guarantee operation from several IoT applications [11].

Important evaluation metrics for the detection of anomalies are precision, retreat, F1 score and precision. The accuracy measures the proportion of anomalies that are properly identified as abnormal cases and focuses on the minimization of false positive. Memory or sensitivity indicates the percentage of real anomalies that have been properly recognized by the model and emphasizes the ability to grasp the real positive. The F1 score combines precision and withdrawal in order to enable a balanced evaluation of the model output in both dimensions. The precision, on the other hand, evaluates general correction if we consider both the real positive and real negative.

The performance analysis is to carry out experiences and simulations for the assessment of ML models under different conditions. Researchers use real data records or simulated environments to demonstrate the capacities of algorithms when recognizing anomalies, whereby factors such as data volume, noise level and calculation resources are taken into account. Comparative studies in several ML techniques help to identify the strengths, weaknesses and the relevance of each model for certain IoT application cases.

In addition, the performance analysis extends to evaluate the way models manage challenges such as unfavorable attacks or changes to the data models over time. Techniques, so that the cross -painting guarantees that the models are robust in new data and generalize well, which minimizes the risk of overlapping and improving reliability in the detection of anomalies.

If you use complete evaluation measures and strict performance analysis, interested parties can make sound decisions about the implementation of anomaly recognition solutions in the intelligent sensors of IoT sensors. These ideas contribute to improving system resilience, optimizing resource management and the weakening of risks that are connected to anomalies in IoT environments and guarantee robust and safe operations in various IoT applications.

VI. CONCLUSION AND FUTURE DIRECTIONS

Automatic learning methods (ML) have changed the panorama of the detection of anomalies in Internet sensor networks (IoT) (Sirn), which enables early identification of unusual behavior or events that can endanger the integrity or performance of the system. Many case studies show the practical applications and the effectiveness of the ML by recognizing anomalies in various IoT sectors.

In industrial IoT environments, ML algorithms are used to monitor devices and machine output and identify differences compared to standard operating models that could display potential failures or maintenance needs. For example, predictive maintenance systems use the ML to analyze data from the manufacturing machine sensor, which facilitates prompt interventions, avoiding expensive deteriorations and improving operating efficiency.

In the field of intelligent medical care, the detection of anomalies that are promoted by ML improves the patient surveillance services and health services significantly. IoT devices continuously collect physiological data, including heart rate, blood pressure and temperature as well as patients. ML models process this data to identify abnormalities that can indicate critical health or irregularities that enable rapid medical reactions and improvement in patient results.

Environmental monitoring is another important area in which ML is essential. IoT sensors in environmental monitoring networks collect data on air quality, pollution levels and climatic conditions. ML algorithms rate these data flows in order to identify unusual models or trends that could mean environmental threats or abnormal changes, which enables quick reactions and reduction strategies.

In addition, the detection of ML anomalies is of crucial

Current Journal of Engineering and Science Research
Volume 2, Issue 2, pp 6-11, February 2025
ISSN (online): 3049-1738
DOI: https://doi.org/10.47001/CJESR/2025.202002
Available Online at https://www.cjesr.com

importance in order to maintain cyber security in IoT implementations. The ML models rate network traffic, user behavior and the interactions of devices to discover suspicious activities or intrusions that differ from typical models. Due to the early detection of security threats, companies can take proactive measures to protect IoT systems from cyber attacks and data offenses.

REFERENCES

[1] D. Ucci, L. Aniello, and R. Baldoni, "Survey of machine learning techniques for malware analysis," Computers & Security, vol. 81, pp.123–147, 2019.

[2] S. M. Tahsien, H. Karimipour, and P. Spachos, "Machine learning based solutions for security of internet of things (iot): A survey," Journal of Network and Computer Applications, vol. 161, p. 102630, 2020.

[3] F. Hussain, R. Hussain, S. A. Hassan, and E. Hossain, "Machine learning in iot security: Current solutions and future challenges," IEEE Communications Surveys & Tutorials, vol. 22, no. 3, pp. 1686–1721, 2020.

[4] D. Gibert, C. Mateu, and J. Planes, "The rise of machine learning for detection and classification of malware: Research developments, trends and challenges," Journal of Network and Computer Applications, vol.153, p. 102526, 2020.

[5] Haque, Ahshanul, et al. "Wireless sensor networks anomaly detection using machine learning: a survey." Intelligent Systems Conference. Cham: Springer Nature Switzerland, 2023.

[6] A.B. Nassif, M. A. Talib, Q. Nassir, H. Albadani, and F. D. Albab, "Ma-chine learning for cloud security: A systematic review," IEEE Access, 2021.

[7] S. Yeom, I. Giacomelli, M. Fredrikson, and S. Jha, "Privacy risk inmachine learning: Analyzing the connection to overfitting," in 2018 IEEE31st Computer Security Foundations Symposium (CSF). IEEE, 2018, pp.268–282.

[8] Bandyopadhyay, Debasis, and Jaydip Sen. "Internet of things: Applications and challenges in technology and standardization." Wireless personal communications 58 (2011): 49-69.

[9] Haji, Saad Hikmat, and Siddeeq Y. Ameen. "Attack and anomaly detection in iot networks using machine learning techniques: A review." Asian J. Res. Comput. Sci 9.2 (2021): 30-46.

[10] JONNERBY, JAKOB, A. BREZGER, and H. WANG. "Machine learning based novel architecture implementation for image processing mechanism." International Journal of communication and computer Technologies 11.1 (2023): 1-9.

[11] Cide, Felip, José Urebe, and Andrés Revera."Exploring Monopulse Feed Antennas for Low Earth Orbit Satellite Communication: Design, Advantages, and Applications." National Journal of Antennas and Propagation 4.2 (2022): 20-27.

[12] G. Sasikala, & G. Satya Krishna. (2023). Low Power Embedded SoC Design. Journal of VLSI Circuits and Systems, 6(1), 25–29. https://doi.org/10.31838/jvcs/06.01.04.

[13] Alghanmi, Nusaybah, Reem Alotaibi, and Seyed M. Buhari. "Machine learning approaches for anomaly detection in IoT: an overview and future research directions." Wireless Personal Communications 122.3 (2022): 2309-2324.

[14] Raghuvanshi, Ajay Singh, Rajeev Tripathi, and Sudarshan Tiwari. "Machine learning approach for anomaly detection in wireless sensor data." International Journal of Advances in Engineering & Technology 1.4 (2011): 47.

[15] K. A. da Costa, J. P. Papa, C. O. Lisboa, R. Munoz, and V. H. C.de Albuquerque, "Internet of things: A survey on machine learning-based intrusion detection approaches," Computer Networks, vol. 151, pp. 147–157, 2019.

[16] Zhang, Hao, et al. "A network anomaly detection algorithm based on semi-supervised learning and adaptive multiclass balancing." The Journal of Supercomputing 79.18 (2023): 20445-20480.

[17] Chatterjee, Ayan, and Bestoun S. Ahmed. "IoT anomaly detection methods and applications: A survey." Internet of Things 19 (2022): 100568.

[18] Al-amri, Redhwan, et al. "A review of machine learning and deep learning techniques for anomaly detection in IoT data." Applied Sciences 11.12 (2021): 5320.

Current Journal of Engineering and Science Research
Volume 2, Issue 2, pp 6-11, February 2025
ISSN (online): 3049-1738
DOI: https://doi.org/10.47001/CJESR/2025.202002
Available Online at https://www.cjesr.com

Citation of this Article:

Swapnil Deshpande. (2025). Automated Machine Learning Methods for Identification of Anomalies in IoT Sensor Networks. *Current Journal of Engineering and Science Research*. 2(2), 6-11. Article DOI: https://doi.org/10.47001/CJESR/2025.202002

***** End of the Article *****