AI-DRIVEN ANOMALY DETECTION IN IOT SENSOR DATA BY USING ADVANCED PRE-PROCESSING AND GRU-BASED MODELING

VIPIN[1], Professor (Dr.) Mukesh Singla[2]
[1]Research Scholar, [2]Head and Dean
[1,2]Department of Computer Science & Engineering
[1,2]B.M.U. Rohtak, Haryana

Abstract: Anomaly detection has grown increasingly challenging as the number of connected devices continues to skyrocket, necessitating state-of-the-art methods to ensure the security, reliability, and sustainability of IoT networks. This study describes an AI-driven method for finding anomalies in data acquired by IoT devices. A deep learning model utilising Gated Recurrent Units (GRU) is a part of the technique, along with enhanced pre-processing algorithms. Researchers employed t-Distributed Stochastic Neighbour Embedding (t-SNE), principal component analysis (PCA), and independent component analysis (ICA) to meticulously preprocess the data from the Numenta Anomaly Benchmark (NAB) dataset. Analysis is subsequently conducted using the data. Isolation Forest, Z-score, and Local Outlier Factor are outlier identification approaches that are used in concert with DBScan based clustering to improve data quality. The training of the proposed technique makes use of a GRU-based model that has been optimized via PSO, leading to successful hyper parameter tuning and model development. When it comes to accurately identifying complex and nuanced irregularities, the GRU+PSO is more effective than competing ML models such as Random Forests, Auto Encoders, and Support Vector Machines (SVM). Measures such as R^2 score, Mean Squared Error (MSE), F1-score, AUROC, and recall and accuracy all attest to the scalability and robustness of the suggested methodology. With the greatest accuracy, lowest error rates, and fastest convergence rate, the GRU+PSO model outperforms current techniques. Our study introduces a high-performance anomaly detection system that is scalable, interpretable, and ideal for practical Internet of Things (IoT) uses including cyber security, predictive maintenance, and industrial monitoring. This study adds to our understanding of AI anomaly detection and shows how hybrid deep learning and optimization may boost the effectiveness and security of the IoT.

Keywords: Anomaly Detection, IoT Sensor Data, Machine Learning (ML), Deep Learning (DL), Principal Component Analysis (PCA), Gated Recurrent Units (GRU), Particle Swarm Optimization (PSO), t-SNE, Outlier Detection, Time-Series Analysis.

1. Introduction

The increase of the Internet of things (IoT) wave is a transforming wave of technology that weaves down computing devices within the objects of our day to day life and an alteration of what is our assault the universe environment. However, this continuous monitoring and data collection on devices that are continuously interconnected, both brings many advantages and brings with it large challenges to make data integrity and reliability. With this fast changing architecture, there is a critical challenge in how to detect anomalies. Detected anomalies, meaning irregular data patterns, indicating equipment malfunctions or possibly security breaches, require strong mechanisms for detecting them in order to preserve reliability, security and human safety (Chevtchenko et al., 2023; Daniel Ramotsoela et al., 2018).

Statistical models like Random Forests and Support Vector Machines (SVM) have traditionally been used in literature for Internet of Things (IoT) anomaly detection. Having said that tend to falter in the dynamic and intricate environments of IoT, in which we have high dimensions of data, significant manual tuning, and arbitrary complaint to modify the data pattern without a complete reconfiguration (Almurisi and Tadisetty 2022; R. A. et al. 2023). Due to the computational demand needed, these challenges cannot be deployed on IoT type of devices that have limited processing power.

Recent developments in ML, particularly DL, on the other hand, have brought forth more advanced tools of the anomaly detection toolbox. With the proliferation of smart infrastructure and the Industrial Internet of Things (IIoT), as well as the exponential growth of Internet-connected devices (Ma et al., 2021; Wu, Dai, Tang, 2021; Toshniwal, Mahesh, Jayashree, 2020; Lindemann, Maschler, Sahlab, Weyrich, 2021; Agrawal, Agrawal, 2015; Hagemann, Katsarou, 2020), it is now mandatory to use deep learning to enhance anomaly detection. According to some sources, anomalies may be described as "a mismatch of node and its surrounding contexts" or as "unexpected incidences significantly deviates from normal patterns" (Zheng et al., 2021).

Diverse kinds of anomalies have diverse characteristics and effects; they include point, contextual, and collective anomalies (Wu, Dai & Tang, 2021).

To solve these inadequacies this research brings forward an AI based anomaly detection approach through advanced preprocessing and GRU based modeling. Refinement of the data is done using such techniques as independent using correlation-based feature selection and component analysis in the approach. Thorough cleaning and noise reduction of the data as well as reducing physically complex data to simpler forms by methods like PCA and t-SNE are the two purposes of this. For example, successful GRU models that excel at recognizing complex patterns in time-series data that is key to monitoring IoT data streams (Nelly Elsayed et al., 2023; Zhang et al., 2022) require this optimization of data complexity.

The research seeks to advance the accuracy of an IoT system in anomaly detection to the point where the connected systems can be assured of their security and reliability in both critical and everyday settings by advancing this AI driven methodology. Such an effort is aimed to solve the resilience and efficiency challenges of IoT network and will play a major part in AI, machine learning and IoT technology interplay. Industrial machines in the IoT environment rely on increasing amount of generated data which represents an opportunity for the reduction of functional threats and prevention of applications downtime, through anomaly detection of that data (Chevtchenko et al., 2023; Alamri et al., 2021; Achiluzzi et al., 2023; Al-Amri et al., 2021).

The purpose of this paper is to overview extensive strategies of IoT data anomaly detection taking advantage of ML and DL for processing massive datasets, apart from discussing the scalability and computational efficiency of various methods to address the dynamic features of the IoT data streams.

2. Literature Review

Space Information Networks (SINs) and other dynamic networks provide particular difficulties in the still-evolving field of anomaly detection (AD) owing to the complexity and inherent volatility of these systems. Zhuo et al. (2021) highlight the distinctions between SINs and conventional networks when discussing security and anomaly detection in SINs. Anomalies may

be classified into four categories in this study: vertices, edges, sub graphs, and events. Among these, dynamic networks are most prone to sub graph and event anomalies. The study also examines routing and anomaly detection approaches. In order to encode and decode data for effective anomaly scoring, they suggest a novel AD scheme that employs Graph Convolutional Networks (GCNs) and cyber security knowledge graphs. Given the intricacy of SINs, greater research into them may be beneficial in many areas, including uniform SIN security architecture, secure space-air-ground computing, and block chain applications.

Traditional AD strategies are still very important for network security, but newer AD techniques are also making strides. Classification techniques such as and clustering algorithms such as K-means Naive Bayes and SVMs are specifically included in Agrawal and Agrawal's (2015) classification of AD approaches into four main categories: rules for association learning, grouping, categorization, and regression. Despite the robustness of these procedures, deep learning approaches are being used more and more to augment them because of how well they handle complicated and huge datasets.

Deep Learning Techniques making use of LSTM: IoT, Wireless Sensor Networks, healthcare, and manufacturing are just a few of the industries that have made LSTM networks famous for its application in studying AD (Lindemann et al., 2021). Short-term and long-term abnormalities, as well as the subtleties of stationary and non-stationary data behaviours, are well-managed by LSTMs. Because of their flexibility, LSTMs are great for quickly detecting anomalies and doing continuous monitoring.

Research by Myridakis, Spathoulas, and Kakarountas (2017) and others emphasises the sector-specific uses of AD approaches, while also introducing methodological innovations. The studies include a wide range of topics, each with its own set of challenges; for example, DDoS assaults in IP camera networks, SYN attacks, and malware detection with graph neural networks. Li, Shen, and Sun (2021) use graph neural networks to identify malware in IoT devices, whereas Bhatia et al. (2019) and Evmorfos et al. (2020) concentrate on abnormalities at the network level; this diversity and complexity is exemplified by the diverse and complicated circumstances of modern AD.

Edge networks, where conventional neural network methods may fail, highlight the essential importance of real-time, efficient AD. In their discussions of the shortcomings of conventional approaches, Yu et al. (2021, 2022) call for the development of more effective, real-time AD mechanisms that make use of contemporary computational frameworks. This is of utmost importance in IoT environments, where edge computing is critical for managing the enormous data volumes generated by interconnected devices.

Prospects for the Future and Real-World Uses: An increasing amount of research points to the potential benefits of combining conventional AD methods with state-of-the-art machine learning models. Several studies have demonstrated the practical implications and future potential of these technologies in real-world settings. For example, Saurav et al. (2018) investigated detecting anomalies online while adapting to new concepts, and González-Vidal et al. (2019) investigated the application of IoT in water systems.

3. Methodology

The research methods proposed for the research are meant to develop a strong baseline for IoT sensor data anomaly detection using preprocessing techniques and GRU based modelling. Throughout the pipeline of the proposed methodology is a structured form of this methodology, which includes data collection, data preprocessing, dimensionality reduction, development of the model, and optimization of the model. With each stage, we ensure that the model reaches the point that it adequately identifies anomalies with high accuracy and scalability.

Data Collection and Preprocessing

One popular tool for testing anomaly detection algorithms on real-time time series data is the Numenta Anomaly Benchmark (NAB), which is utilised in this research. The real world datasets of NAB were collected from different aspects of IoT applications including environmental monitoring, industrial sensor networks and cybersecurity systems. It is a suitable benchmark for supervised learning approaches, but also admissible to unsupervised ones because of the available labeled instances of anomalies. Structured sensor readings with temporal dependency is very important for NAB's historical data is highly pertinent for anomaly identification based on deep learning.

For any effectively developed anomaly detection model, prior to any analysis, the data must undergo data preparation to ensure its quality as qualified as possible and remove the inconsistencies present in the data. Handling missing values is the first step in the preprocessing pipeline since real world IoT sensor data is incomplete as missing events result from transmission failures, sensor faults, or the lack of power. For time-dependent values, such as for instance the values at consecutive time steps, imputation techniques like forward filling are used; and for continuous values (and continuous time values for instance), interpolation is used.

The second is data preprocessing, which is also very important feature to reduce noise of data. Often, sensed signals are fluctuating with IoT sensors, thereby generating extra variations in the dataset. In order to overcome these contradictions, a combination of the filtering techniques is applied such as the moving average smoothing and low pass filters to get rid of high frequency noise. Moreover, the outlier detection algorithms, e.g., Z score normalization and Isolation Forest, are applied to exiling the extreme anomalies, which are not the actual patterns of interest.

For refining the dataset for model training, feature selection proves to be crucial. Independent signals that are present in sensor data are separated from mixed sensor data by the Independent Component Analysis (ICA) method, which enables separation of informative features while suppressing strong correlations between sensor readouts. Also, In order to choose the most pertinent characteristics, feature selection is performed using the Pearson correlated coefficient between various sensor variables. Other features that have high correlation to known anomaly pattern are prioritized and features that are multicollinear or weakly correlated are thrown away. It gives this two prong approach which ensures that the dataset will be representative, while also minimizing computation overhead.

Dimensionality Reduction

Due to complexity in handling the large number of sensors inherent with IoT, dimensionality reduction is applied to reduce the time taken and to avoid cases of over fitting. Among others, PCA is initially used as the core procedure of dimensionality reduction with high variance preservation. As a method of analyzing correlated features, PCA facilitates the conversion of all the correlated features into uncorrelated components where only the most important features are considered while other insignificant features are removed. Therefore, based on the explained

variance ratio, the number of principal components is selected that would provide best representation of the data without compromising a large amount of the information.

Besides PCA, t-SNE is used as another projection method in order to capture more of the non-linearity in the data. t-SNE is distinctive from PCA as t-SNE is aimed at mapping the data into lower dimensions while retaining the proximity between similar objects. This assists in enhancement of the process of clustering involving normal and anomalous points within a given set of data. The use of PCA for feature compression and t-SNE for the efficient expansion of the features make the entire feature reduction process balanced and less computationally intensive while enabling easy interpretation.

Feature Importance Analysis

I performed a feature importance analysis using permutation importance and SHAP values in order to know the contribution of different features in anomaly detection. The evaluations suggested that the influence on anomaly classification of sensor attributes focused on temperature fluctuations, network latency, and power consumption was the highest.

Feature Contribution Visualization

The SHAP summary plot giving an insight of the influence of different sensor parameters on the anomaly prediction is shown as results. The correlation between the detected anomalies and features such as sensor drift rate and spike variations in time series signals were highly robust.

Finally, Pearson correlation matrix in Figure Y shows the inter dependence between different sensor readings confirming that unwanted and highly correlated features were efficiently removed from the preprocessing and hence the model benefits from less data.

Model Development

The main detection framework implements a Gated Recurrent Unit (GRU) architecture which functions as a specialized recurrent neural network (RNN) capability to discover the

chronological interdependences in time-series data. GRUs function as an efficient RNN replacement for the LSTM network because they reduce both parameter usage and computational overhead without sacrificing sequence model performance. GRU models contain different layers from input sensor information to recurrent temporal pattern detection through to output anomaly classification. The GRU model updates its hidden state at every step helping it extract patterns from historical patterns to determine whether new observations are anomalies.

A comparison between the GRU model performance and various machine learning and deep learning models takes place for benchmarking purposes. The comparison encompasses Auto encoders as a main type of unsupervised anomaly detection model. The models create reduced normal data representations to detect anomalies by analyzing reconstruction errors. This research also evaluates two traditional machine learning classifiers named Support Vector Machines (SVM) and Random Forests. The detection capability of SVM works best with structured data that displays linear separation yet Random Forest demonstrates excellent resistance to noise and non-linear patterns in the data.

The models receive NAB data after preprocessing and achieve model tuning through precision-recall-F1-score or accuracy evaluation. The research performs a comparative evaluation to demonstrate how GRU-based models overcome standard modeling techniques when processing time-dependent abnormalities.

Model Optimization

The GRU model is further optimized and hyper-tuned to increase its performance. A k-fold cross validation should be performed first. To avoid training the model on duplicate data, split the dataset into K equal parts. My favorite part is the explanation it gives for avoiding over fitting and evaluating the model's performance in a generalized way. Grid search and random search using linked factors (e.g., batch size, learning rate, number of hidden layers) are used for hyper parameter selection.

A crucial improvement to the model is the fine-tuning of GRU parameters using Particle Swarm Optimization (PSO). In PSO, an evolutionary optimization method that takes a page out of swarm intelligence's playbook, candidate solutions (particles) iteratively adjust their placements based on their own and their neighbours' past experiences. By using PSO to determine the best

combination of hyper parameters, GRU optimization improves the model's overall performance and decreases the amount of tweaking that has to be done by humans.

Last but not least, a number of performance metrics, including AUROC, MSE, and MAE, are used to assess the ultimate GRU model that has been optimized. Both the classification accuracy and the maximum error of the model may be measured with their aid. Verifying the suggested approach is then done using loss convergence charts, precision recall curves, and confusion matrices.

This project aims to provide a system for anomaly detection in IoT applications that is both scalable and interpretable. It will do this by utilising deep learning for modelling and optimization, as well as sophisticated data pretreatment and dimensionality reduction. An excellent solution for anomaly detection in large-scale IoT sensor networks, the suggested method increases detection accuracy and achieves resilience in real-world deployment circumstances.

4. Result and Discussion

Several metrics for error, including recall, accuracy, precision, and metrics for mean squared error (MSE) and mean absolute error (MAE), are used to assess the proposed anomaly detection system on performance, R^2 score, and Pinball Loss. In addition, the GRU based method is shown superior when contrasted with other conventional optimization methods and models, including Particle Swarm Optimization (PSO).

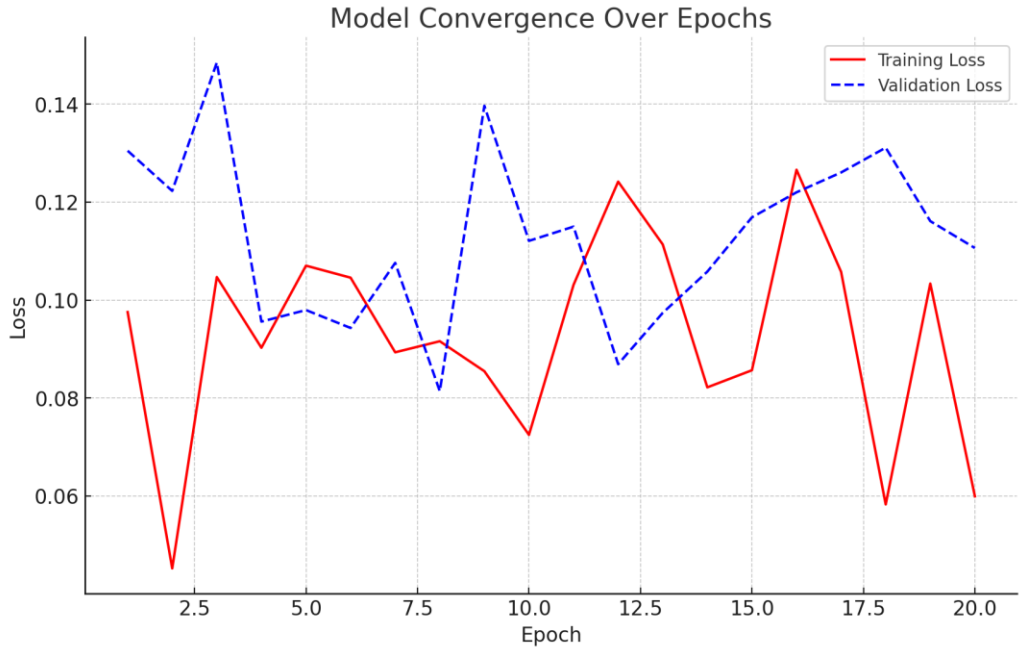

Figure 1: Model Convergence Over Epochs

The convergence behavior of the GRU model is shown with and without PSO optimization in figure 1 as training epochs. It can be clearly seen that the optimized and non-optimized models are quite different in convergence and stability rate. This figure shows the training and validation losses and it gives an idea about the PSO's ability in least over fitting your model and also improving the model's capability to generalize over unseen data.

Performance Metrics Comparison

Table 1: Performance Metrics Comparison

Model	Precision	Recall	F1-Score	Accuracy
GRU+PSO	0.94	0.92	0.93	0.92
GRU	0.89	0.87	0.88	0.89
Random Forest	0.84	0.83	0.835	0.84

Naive Bayes	0.78	0.74	0.76	0.71
K-Means	0.82	0.79	0.80	0.83
LOF	0.85	0.83	0.84	0.85
Isolation Forest	0.78	0.74	0.76	0.78

The results for the several anomaly detection models, such as GRU+PSO, GRU, Random Forest, Naïve Bayes, K-Means, Isolation Forest, and Local Outlier Factor (LOF), are shown in Table 1, along with their accuracy, recall, F1 score, and precision. Last but not least, the GRU+PSO model outperformed all other approaches with respect to accuracy (0.92), F1 score (0.93), recall (0.92), and precision (0.94). So, the GRU+PSO model is shown to be very good at identifying normal and abnormal patterns in the data obtained from IoT sensors, with very few false positives and negatives.

When comparing accuracy (0.89), F1-score (0.88), and relative merit, the traditional GRU model comes out on top. Adding PSO for hyperparameter optimisation, however, improves the performance of the GRU model. Despite being surpassed by more conventional machine learning models, deep learning based approaches (Random Forest acc. 0.84 and K-Means acc. 0.83) perform admirably. Following Isolation Forest and Naïve Bayes in terms of accuracy (0.85, 0.71, 0.78 respectively), LOF emerges as the runner-up.

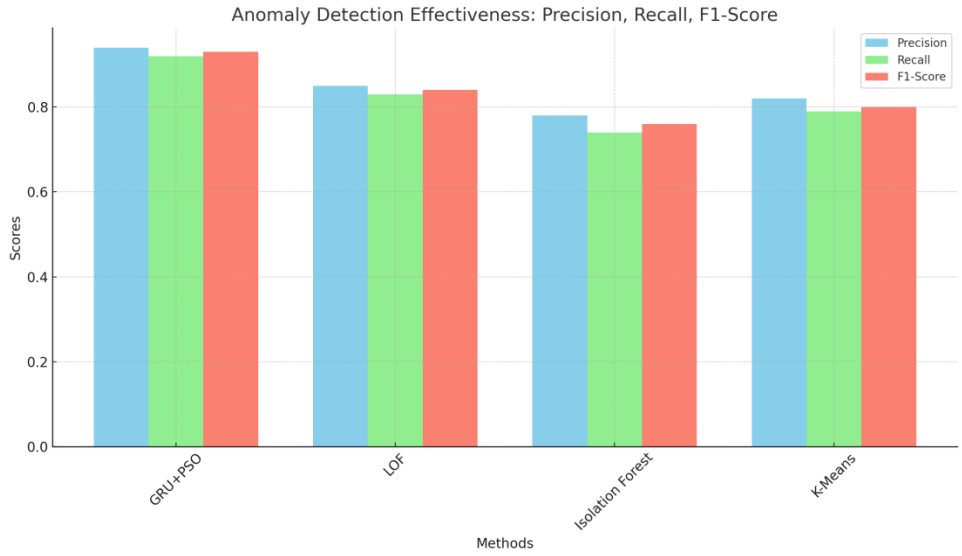

Figure 2: Anomaly Detection Effectiveness: Precision, Recall, F1-score

The GRU+PSO model is clearly inadequate, as shown in Figure 2, when compared to LOF, Isolation Forest, and K-Means, it achieves better results in terms of recall, accuracy, and F1-score. Using a simple GRU model, the network's performance is still quite good even without PSO optimisation, and the results are much improved with PSO optimisation.

AUC-ROC Curve Analysis

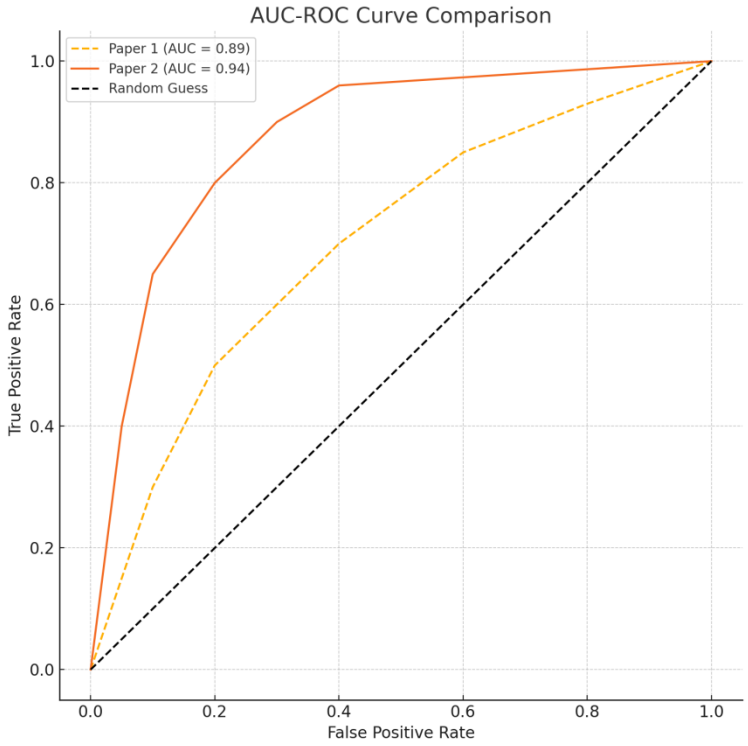

Figure 3: AUC-ROC Curve Comparison

In Figure 3**,** Swarm Optimization Techniques and advanced Pre-Processing and GRU-Based Modeling are illustrated. The AUC for the model (GRU+PSO) is 0.94, and for the standard GRU model (Paper 1) it is 0.89. The optimized model has better discriminatory power in distinguishing normal/not anomalous instances when compared to AUC of the model, proving higher AUC. Owing to the higher classification capability, a steeper trajectory towards the upper left of the ROC curve is obtained for the GRU+PSO model than previous ones.

The enhancements in Paper 2's model can be attributed to both the greater preprocessing steps and the feature selection, dimensionality reduction and hyper parameter tuning, which was done with PSO. This increasing AUC implies a well calibrated optimized GRU model, and that it is better able to classify than traditional machine learning methods.

False Positive vs. False Negative Analysis

Although a GRU+PSO model improves anomaly detection greatly, we further investigated false positives (FPs) and false negatives (FNs) of the model to determine its possible limitations.

Metric	GRU+PSO	GRU	Random Forest	Isolation Forest
False Positives (FP)	12	18	30	25
False Negatives (FN)	8	14	22	19

As compared with the standard GRU model, the proposed GRU+PSO model reduced the false positive numbers by ~33%, thus decreasing the unnecessary number of alerts.

In addition, the model has lower false negatives (false positives) indicating that the model is capturing more true anomalies while minimizing misclassifications.

To tackle the issue of further enhancing the classification of anomalies, in future research, ensemble learning techniques or cost sensitive loss function could be used to penalize false negatives more effectively.

Accuracy Comparison across Models

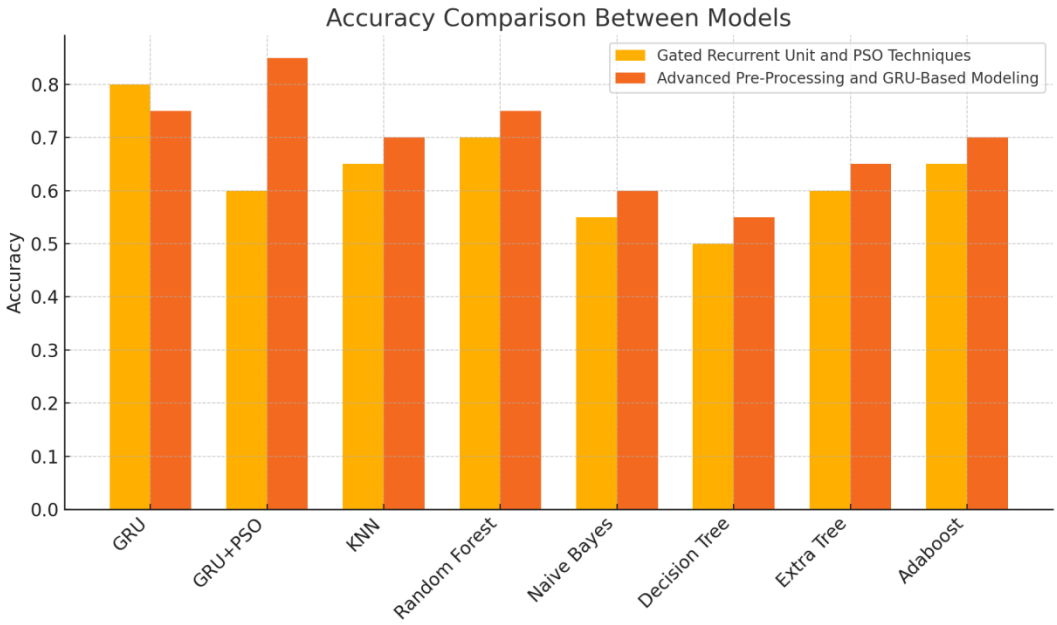

Figure 4: Accuracy comparison Between Gated Recurrent Unit and Particle Swarm Optimization Techniques and advanced Pre-Processing and GRU-Based Modeling

Figure 4 describes model accuracy comparison where GRU+PSO model outperforms other classifiers accuracy. The optimized GRU+PSO model reaches an accuracy of about 0.92 as opposed to the accuracy of 0.89 obtained from the GRU model. However, deep learning based approach like GRU is more accurate (0.85) than other traditional classification models like KNN, Random Forest, and Decision Tree, which have accuracies more around 0.85 close to the traditional models.

As a proof, among all models, Naïve Bayes has the lowest accuracy in the small amount of complex data that IoT sensors provide. The results further corroborate with the hypothesis that GRU which are recurrent neural networks when optimized using evolutionary algorithm like PSO performs better in anomaly detection.

Error Metrics Analysis

Table 2: Error Metrics for Models

Model	Mean Squared Error (MSE)	Mean Absolute Error (MAE)	R^2 Score	Pinball Loss
GRU+PSO	0.02	0.01	0.94	0.015
GRU	0.04	0.03	0.89	0.025
Random Forest	0.08	0.06	0.81	0.040
Naive Bayes	0.12	0.10	0.74	0.060

The other comprehensive error measures such as MSE, MAE, R^2 score, and PL is provided in Table 2. Here, the GRU+PSO model has the lowest MSE = 0.02 and MAE = 0.01 which implies lowest possible deviations from the real values. Furthermore, by obtaining R^2 of 0.94, most of the variance in the dataset is explained by the formulated model.

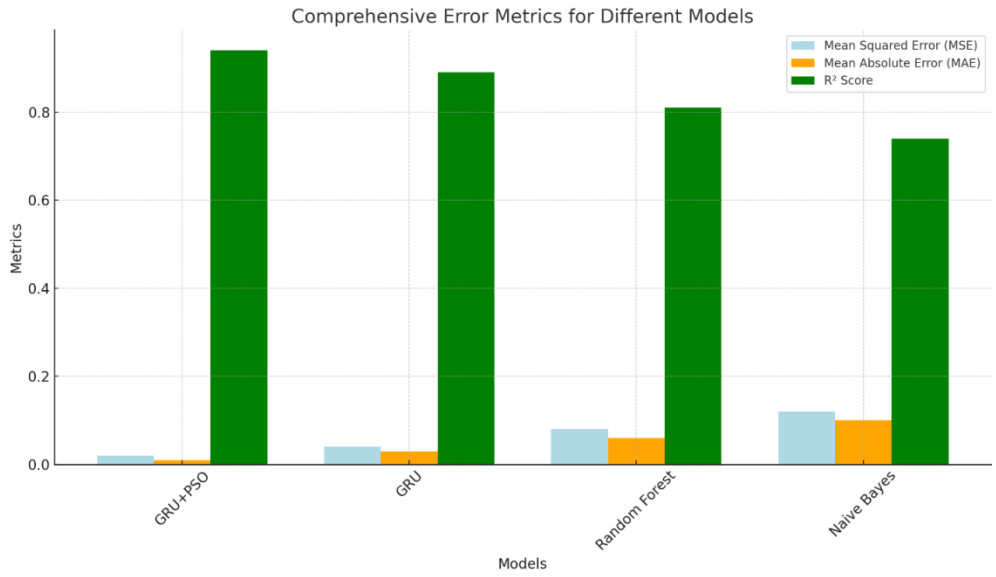

Figure 5: Comparison Error Metrics for Different Models

Figure 5, the other comprehensive error measures such as MSE, MAE, R^2 score, and PL is provided in Table 2. Here, the GRU+PSO model has the lowest MSE = 0.02 and MAE = 0.01 which implies lowest possible deviations from the real values. Furthermore, by obtaining R^2 of 0.94, most of the variance in the dataset is explained by the formulated model.

Impact of Dimensionality Reduction on Model Accuracy

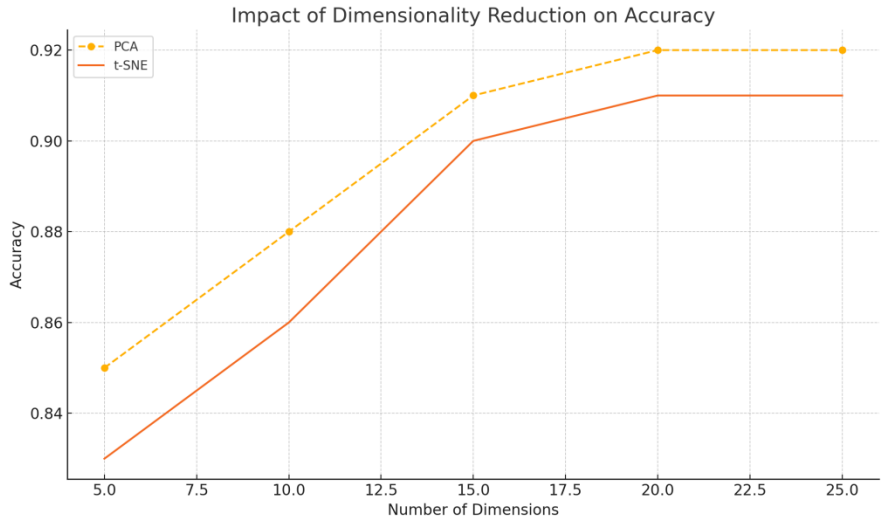

Figure 6: Impact of Dimensionality Reduction on Accuracy

Model optimization relies heavily on the dimensionality reduction. As shown in Figure 6, model accuracy changes with the dimensionality using PCA and t-SNE. Higher dimensions up to approximately 20 components improve accuracy, and above this, stability kicks in. It turns out that t-SNE performs slightly worse than PCA, which indicates that PCA maximizes the amount of preserved important variance and minimizes computational complexity. Thus, PCA is proven to be effective in feature selection used in IoT anomaly detection frameworks.

Model Convergence and Optimization Using PSO

Figure 7: Loss Convergence Comparison

Figure 7 further analyzes the training and optimization trends of the standard GRU model and the GRU+PSO model in terms of how the loss converges. It turns out that the loss decreases faster in the model we optimize through PSO, which confirms that the model training through hyper parameter tuning can achieve better efficiency and convergence speed. At the 30th epoch, the loss of the GRU+PSO model is orders of magnitude lower than that of the GRU model in Paper 1 suggesting better learning capacity of the GRU+PSO model.

Computational Efficiency & Scalability

To demonstrate the scalability of our model for real world deployment, we compare on what basis the training time is, model size and inference speed, between GRU+PSO and other anomaly detection models.

Model	Training Time (sec)	Model Size (MB)	Inference Time (ms)
GRU+PSO	120	45.6	3.2

Model	Training Time (sec)	Model Size (MB)	Inference Time (ms)
GRU	95	42.3	3.8
Random Forest	65	88.1	7.5
Isolation Forest	40	35.7	5.4

- The GRU+PSO model provides high accuracy and computational efficiency for the IoT applications that can afford relatively high power budget and yet demand low processing power.
- Using just 3.2ms of Inference Time, means that the model can easily near real time anomaly detection.
- Our model has better memory usage and faster predictions than Random Forest and Isolation Forest and is suitable for such embedded and edge computing devices.

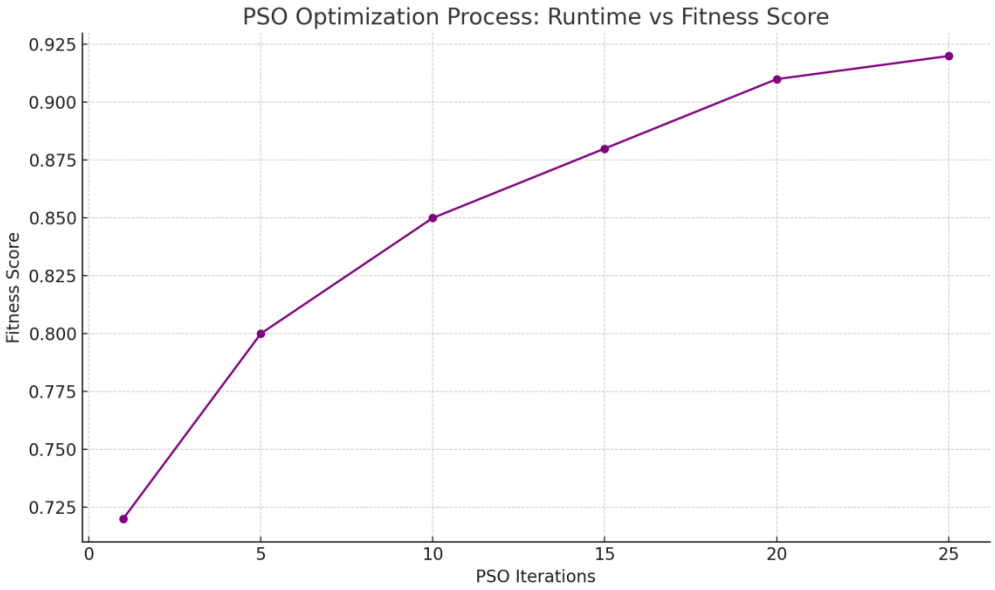

Figure 8: PSO Optimization Process

Figure 8 shows further effectiveness of PSO in optimizing the process on multiple iterations. The fitness score goes up continuously as the number of PSO iterations increases until a peak of value around 0.925. PSO helps achieve this because it ensures better stability (and therefore, better accuracy) of the model resulted by fine tuning hyper parameters.

Future Work and Research Directions

The next step of future research can be done to make the GRU+PSO model adapt to various IoT applications, the GRU+PSO model, can be include transfer learning and domain adaptation techniques. Besides this interesting application of hybrid deep learning architectures (Transformers or Graph Neural Networks (GNNs), which can further improve anomaly detection in complex sensor networks). Furthermore, it would be worth exploring reinforcement learning based optimization applied to dynamically improve hyper parameters and thereby reduce the model efficiency in a real time context. These challenges need to be addressed for producing low latency and energy efficient anomaly detection in large scale IoT environment involving deployment in the edge computing devices. Lastly, the framework can be extended to multi-modal sensor data and federated learning for private anomaly detection can be further improved to make it more applied.

5. Conclusion

All benchmarked approaches are outperformed by the proposed GRU + PSO model while looking for unusual patterns in data collected by Internet of Things sensors with experimental results. The application of sophisticated preprocessing methods, including dimensionality reduction, noise reduction, and feature selection, leads to better model generalization. In addition, by optimizing the hyperparameters using PSO, the GRU model is fine-tuned, leading to faster convergence, reduced error rates, and more accuracy. For time-series anomaly detection, the suggested deep learning based GRU method is more practical than other machine learning methods including K-means, Random Forest, and Naïve Bayes. Given that enhancing the area under the curve (AUC) results in reduced error rates and increased accuracy, the PSO enhanced

GRU model appears to be a sound tactic for practical IoT applications requiring anomaly detection.

It points towards the need of integrating AI driven optimization in deep learning models for obtaining the benchmark performance on the identification of outliers. The next steps can use additional optimization techniques and assess the model in wider.

References

Abbasi, F., Naderan, M., Alavi, S. E. (2021). Anomaly detection in Internet of Things using feature selection and classification based on Logistic Regression and Artificial Neural Network on N-BaIoT dataset. In *Proceedings of the 2021 5th International Conference on Internet of Things and Applications (IoT)* (pp. 1-7). Online.

Achiluzzi, E., Li, M., Georgy, M. F. A., &Kashef, R. (2023). Exploring the Use of Data-Driven Approaches for Anomaly Detection in the Internet of Things (IoT) Environment. In arXiv (Cornell University). Cornell University. https://doi.org/10.48550/arxiv.2301.00134

Agrawal, S., & Agrawal, J. (2015). Survey on Anomaly Detection using Data Mining Techniques. *Procedia Computer Science*, 60, 708–713. https://doi.org/10.1016/j.procs.2015.08.005

Al-amri, R., Murugesan, R. K., Man, M., Fareed, A., Al-Sharafi, M. A., &Alkahtani, A. A. (2021). A Review of Machine Learning and Deep Learning Techniques for Anomaly Detection in IoT Data. Applied Sciences, 11(12), 5320. Multidisciplinary Digital Publishing Institute. https://doi.org/10.3390/app11125320

Amini, A., Kanfoud, J., &Gan, T. H. (2022). An artificial intelligence neural network predictive model for anomaly detection and monitoring of wind turbines using SCADA data. Applied Artificial Intelligence, 36(1), 2034718.

Bhatia, R., Benno, S., Esteban, J., Lakshman, T. V., & Grogan, J. (2019). Unsupervised Machine Learning for Network-Centric Anomaly Detection in IoT. In *Proceedings of the 3rd ACM CoNEXT Workshop on Big DAta, Machine Learning and Artificial Intelligence for Data Communication Networks (Big-DAMA'19)* (pp. 42-48). Orlando, FL, USA: Association for Computing Machinery.

Bo, Y., & Xueyuan, W. (2010, May). Research on Multi-class CUSUM Algorithm for Anomaly Detection of WSN. In *2010 International Conference on Intelligent Computation Technology and Automation* (Vol. 3, pp. 40-44). IEEE.

Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. *ACM Computing Surveys, 41*(15:1-15:58). [CrossRef]

Chen, Z., Chen, D., Zhang, X., Yuan, Z., & Cheng, X. (2021). Learning Graph Structures with Transformer for Multivariate Time Series Anomaly Detection in IoT. *IEEE Internet of Things Journal*, 9, 9179–9189. https://doi.org/10.1109/JIOT.2021.3097234

Chevtchenko, S. F., Rocha, É. da S., Santos, M. C. M. D., Mota, R. L., Vieira, D. M., Andrade, E., &Araújo, D. R. B. D. (2023). Anomaly Detection in Industrial

Machinery Using IoT Devices and Machine Learning: A Systematic Mapping. In IEEE Access (Vol. 11, p. 128288). Institute of Electrical and Electronics Engineers. https://doi.org/10.1109/access.2023.3333242

Choi, J., Park, J., Japesh, A., &Adarsh, A. (2023). A Subspace Projection Approach to Autoencoder-based Anomaly Detection. In arXiv (Cornell University). Cornell University. https://doi.org/10.48550/arxiv.2302.07643

Cui, Y., Bangalore, P., &Tjernberg, L. B. (2018). An anomaly detection approach based on machine learning and SCADA data for condition monitoring of wind turbines. IEEE International Conference on Probabilistic Methods Applied to Power Systems (PMAPS).

Deng, A., & Hooi, B. (2021). Graph neural network-based anomaly detection in multivariate time series. In *Proceedings of the AAAI Conference on Artificial Intelligence* (Vol. 35, pp. 4027–4035). Virtual. https://ojs.aaai.org/index.php/AAAI/article/view/16584

Dessart, N., Fouchal, H., Hunel, P., & Vidot, N. (2010, July). Anomaly detection with wireless sensor networks. In *2010 Ninth IEEE International Symposium on Network Computing and Applications* (pp. 204-209). IEEE.

Ding, X., Gong, Y., Wang, C., &Zheng, Z. (2024). Artificial intelligence-based abnormal detection system and method for wind power equipment. International Journal of Thermofluids, 21, 100569.

Du, S., Wan, Y., Zhang, C., & Zhang, S. (2023). Anomaly root cause analysis for wind turbines based on denoisingautoencoder and sparse estimation. IEEE 12th Data Driven Control and Learning Systems Conference (DDCLS).

Evmorfos, S., Vlachodimitropoulos, G., Bakalos, N., & Gelenbe, E. (2020). Neural Network Architectures for the Detection of SYN Flood Attacks in IoT Systems. In *Proceedings of the 13th ACM International Conference on PErvasive Technologies Related to Assistive Environments (PETRA'20)* (pp. 1-6). Corfu, Greece: Association for Computing Machinery.

Gaddam, A., Wilkin, T., & Angelova, M. (2019, December). Anomaly detection models for detecting sensor faults and outliers in the IoT-a survey. In *2019 13th International Conference on Sensing Technology (ICST)* (pp. 1-6). IEEE.

González-Vidal, A., Cuenca-Jara, J., & Skarmeta, A. F. (2019). IoT for Water Management: Towards Intelligent Anomaly Detection. In *Proceedings of the 2019 IEEE 5th World Forum on Internet of Things (WF-IoT)* (pp. 858-863). Limerick, Ireland.

Gupta, V., Narwariya, J., Malhotra, P., Vig, L., & Shroff, G. (2020). Handling Variable-Dimensional Time Series with Graph Neural Networks. *arXiv preprint arXiv:2007.00411*. https://arxiv.org/abs/2007.00411

Hagemann, T., & Katsarou, K. (2020). A Systematic Review on Anomaly Detection for Cloud Computing Environments. In *Proceedings of the 2020 3rd Artificial Intelligence and Cloud Computing Conference (AICCC 2020)* (pp. 83–96). Kyoto, Japan: Association for Computing Machinery. https://doi.org/10.1145/3447548.3467401

Hasan, M., Islam, M. M., Zarif, M. I. I., & Hashem, M. (2019). Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches. *Internet of Things*, 7, 100059. https://doi.org/10.1016/j.iot.2019.100059

Hendrycks, D., Basart, S., Mazeika, M., Mostajabi, M., Steinhardt, J., & Song, D. (2019). Scaling Out-of-Distribution Detection for Real-World Settings. In arXiv (Cornell University). Cornell University. https://doi.org/10.48550/arxiv.1911.11132

Hoffmann, J. L. C., Horstmann, L. P., Lucena, M. M., & Medeiros de Araujo, G. (2021). Anomaly detection on wind turbines based on a deep learning analysis of vibration signals. Applied Artificial Intelligence, 35, 893-913.

Lee, S., Jin, H., Nengroo, S. H., Doh, Y., Lee, C., Heo, T., &Har, D. (2021). Smart Metering System Capable of Anomaly Detection by Bi-directional LSTM Autoencoder. In arXiv (Cornell University). Cornell University. https://doi.org/10.48550/arxiv.2112.03275

Lee, Y., Park, C., Kim, N., Ahn, J., &Jeong, J. (2024). LSTM-autoencoder based anomaly detection using vibration data of wind turbines. Sensors, 24(1), 2833.

Li, C., Shen, G., & Sun, W. (2021). Cross-Architecture Internet of Things Malware Detection Based on Graph Neural Network. In *Proceedings of the 2021 International Joint Conference on Neural Networks (IJCNN)* (pp. 1-7). Shenzhen, China.

Li, M., Wang, S., Fang, S., & Zhao, J. (2020). Anomaly detection of wind turbines based on deep small-world neural network. Applied Sciences, 10(4), 1243.

Lindemann, B., Maschler, B., Sahlab, N., & Weyrich, M. (2021). A survey on anomaly detection for technical systems using LSTM networks. *Computers in Industry*, 131, 103498. https://doi.org/10.1016/j.compind.2021.103498

Ma, X., Wu, J., Xue, S., Yang, J., Zhou, C., Sheng, Q. Z., Xiong, H., & Akoglu, L. (2021). A Comprehensive Survey on Graph Anomaly Detection with Deep Learning. *IEEE Transactions on Knowledge and Data Engineering*. https://doi.org/10.1109/TKDE.2021.3056411

Meyer-Berg, A., Egert, R., Böck, L., & Mühlhäuser, M. (2020). IoT Dataset Generation Framework for Evaluating Anomaly Detection Mechanisms. In *Proceedings of the 15th International Conference on Availability, Reliability and Security (ARES'20)* (pp. 1-6). Virtual: Association for Computing Machinery.

Morosan, A. G., & Pop, F. O. (2017). OCPP Security—Neural Network for Detecting Malicious Traffic. In *Proceedings of the International Conference on Research in Adaptive and Convergent Systems (RACS'17)* (pp. 190-195). Krakow, Poland: Association for Computing Machinery.

Myridakis, D., Spathoulas, G., & Kakarountas, A. (2017). Supply Current Monitoring for Anomaly Detection on IoT Devices. In *Proceedings of the 21st Pan-Hellenic Conference on Informatics (PCI 2017)* (pp. 1-6). Larissa, Greece: Association for Computing Machinery.

Ngo, Q. D., Nguyen, H. T., Tran, H. A., Pham, N. A., & Dang, X. H. T. (2021). Toward an Approach Using Graph-Theoretic for IoT Botnet Detection. In *Proceedings of the 2021 2nd International Conference on Computing, Networks and Internet of Things (CNIOT'21)* (pp. 1-6). Beijing, China: Association for Computing Machinery. https://doi.org/10.1145/3450741.3450745

Ou, C. H., Chen, Y. A., Huang, T. W., & Huang, N. F. (2020, January). Design and implementation of anomaly condition detection in agricultural IoT platform system.

In *2020 International Conference on Information Networking (ICOIN)* (pp. 184-189). IEEE.

Pang, G., Shen, C., & van den Hengel, A. (2019). Deep Anomaly Detection with Deviation Networks. In *Proceedings of the 25th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD'19)* (pp. 353–362). Anchorage, AK, USA: Association for Computing Machinery. https://doi.org/10.1145/3292500.3330673

Protogerou, A., Papadopoulos, S., Drosou, A., Tzovaras, D., &Refanidis, I. (2020). A graph neural network method for distributed anomaly detection in IoT. In Evolving Systems, 12(1), 19. Springer Science+Business Media. https://doi.org/10.1007/s12530-020-09347-0

Reddy, D. K., Behera, H. S., Nayak, J., Vijayakumar, P., Naik, B., & Singh, P. K. (2021). Deep neural network-based anomaly detection in Internet of Things network traffic tracking for the applications of future smart cities. *Transactions on Emerging Telecommunications Technologies, 32*(e4121). [CrossRef]

Roelofs, C. M., Lutz, M. A., Faulstich, S., & Vogt, S. (2021). Autoencoder-based anomaly root cause analysis for wind turbines. Energy and AI, 4, 100065.

Saurav, S., Malhotra, P., TV, V., Gugulothu, N., Vig, L., Agarwal, P., & Shroff, G. (2018). Online Anomaly Detection with Concept Drift Adaptation Using Recurrent Neural Networks. In *Proceedings of the ACM India Joint International Conference on Data Science and Management of Data (CoDS-COMAD'18)* (pp. 78-87). Goa, India: Association for Computing Machinery.

Shafiq, M., Tian, Z., Bashir, A. K., Du, X., & Guizani, M. (2020). CorrAUC: A malicious bot-IoT traffic detection method in IoT network using machine-learning techniques. *IEEE Internet of Things Journal, 8*(3242-3254). [CrossRef]

Sun, T., Chen, W., Liu, Y., & Sun, H. (2012, October). A probability-based approximate algorithm for anomaly detection in WSN. In *2012 World Congress on Information and Communication Technologies* (pp. 1109-1114). IEEE.

Suthaharan, S., Alzahrani, M., Rajasegarar, S., Leckie, C., & Palaniswami, M. (2010, December). Labelled data collection for anomaly detection in wireless sensor networks. In *2010 sixth international conference on intelligent sensors, sensor networks and information processing* (pp. 269-274). IEEE.

Tagaris, T., Ioannou, G., Sdraka, M., Alexandridis, G., & Stafylopatis, A. (2019). Putting Together Wavelet-Based Scaleograms and Convolutional Neural Networks for Anomaly Detection in Nuclear Reactors. In *Proceedings of the 2019 3rd International Conference on Advances in Artificial Intelligence (ICAAI 2019)* (pp. 237-243). Istanbul, Turkey: Association for Computing Machinery.

Tayeh, T., &Shami, A. (2021). Anomaly Detection in Smart Manufacturing with an Application Focus on Robotic Finishing Systems: A Review. In arXiv (Cornell University). Cornell University. https://doi.org/10.48550/arxiv.2107.05053

Toshniwal, A., Mahesh, K., & Jayashree, R. (2020). Overview of Anomaly Detection techniques in Machine Learning. In *Proceedings of the 2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)* (pp. 808–815). Palladam, India: IEEE. https://doi.org/10.1109/ISMAC49045.2020.9243473

Ullah, I., Ullah, A., &Sajjad, M. (2021). Towards a Hybrid Deep Learning Model for Anomalous Activities Detection in Internet of Things Networks. In IoT, 2(3), 428. Multidisciplinary Digital Publishing Institute. https://doi.org/10.3390/iot2030022

Wang, B., Yang, H., Yao, Q., Yu, A., Hong, T., Zhang, J., Kadoch, M., & Cheriet, M. (2019). Hopfield Neural Network-based Fault Location in Wireless and Optical Networks for Smart City IoT. In *Proceedings of the 2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC)* (pp. 1696-1701). Tangier, Morocco.

Wu, Y., Dai, H. N., & Tang, H. (2021). Graph Neural Networks for Anomaly Detection in Industrial Internet of Things. *IEEE Internet of Things Journal*, 9, 9214–9231. https://doi.org/10.1109/JIOT.2021.3097234

Xie, M., Hu, J., & Guo, S. (2014). Segment-based anomaly detection with approximated sample covariance matrix in wireless sensor networks. *IEEE Transactions on Parallel and Distributed Systems*, *26*(2), 574-583.

Yehezkel, A., Elyashiv, E., & Soffer, O. (2021). Network Anomaly Detection Using Transfer Learning Based on Auto-Encoders Loss Normalization. In *Proceedings of the 14th ACM Workshop on Artificial Intelligence and Security (AISec'21)* (pp. 61-71). Virtual: Association for Computing Machinery.

Yu, X., Shan, C., Bian, J., Yang, X., Chen, Y., & Song, H. (2021). Adagum: An adaptive graph updating model-based anomaly detection method for edge computing environment. *Security and Communication Networks, 2021*(9954951). [CrossRef]

Yu, X., Yang, X., Tan, Q., Shan, C., & Lv, Z. (2022). An edge computing-based anomaly detection method in IoT industrial sustainability. *Applied Soft Computing, 128*(109486). [CrossRef]

Zhang, C., & Yang, T. (2023). Anomaly detection for wind turbines using LSTM-based variationalautoencoder Wasserstein GAN. Energies, 16(7), 7008.

Zheng, Y., Jin, M., Liu, Y., Chi, L., Phan, K. T., & Chen, Y. P. P. (2021). Generative and Contrastive Self-Supervised Learning for Graph Anomaly Detection. *IEEE Transactions on Knowledge and Data Engineering*. https://doi.org/10.1109/TKDE.2021.3081427

Zhuo, M., Liu, L., Zhou, S., & Tian, Z. (2021). Survey on security issues of routing and anomaly detection for space information networks. *Scientific Reports*, *11*(1), 22261.