# Intelligent Time Series Anomaly Detection in IoT Using Feature Extraction and Hybrid Classification

Srimaan Yarram
Independent Researcher
srimaan.yarram@gmail.com

Srinivasa Rao Bittla
Independent Researcher
sbittla@gmail.com

## Abstract

IoT cyberattacks are becoming more frequent and complicated, threatening individuals and organizations. IoT networks are vulnerable to internal and external cyberattacks because to their openness and self-configuration. DoS attacks are particularly destructive, stopping genuine users from accessing key services. Traditional anomaly detection approaches fail to identify complex temporal correlations and are inaccurate and not robust.

This study introduces a feature extraction-based VGGNet model for time series anomaly detection using the Artificial Butterfly Optimization (ABO) algorithm for feature selection and a hybrid Capsule Network (CapsNet) deep learning model for accurate attack classification. VGGNet extracts hierarchical temporal features to improve representation quality, whereas ABO effectively picks the most relevant features to reduce computing cost. The hybrid CapsNet classifier captures spatial and hierarchical connections among selected characteristics to improve anomaly detection accuracy.

Experimental results on MSL and PSM time series datasets show high classification accuracy, reduced false alarms, and improved precision-recall metrics, exceeding conventional methods. This scalable, adaptable approach detects anomalies in real time, enabling deep learning-driven cybersecurity solutions.

**Keywords:** Denial of Service; Internet of Things; Cybersecurity; Artificial Butterfly Optimization; Hybrid CapsNet; Anomaly Detection.

## 1. Introduction

Through the incorporation of advanced sensors, communication technology, and data analytics, the Industrial Internet of Things (IIoT) has revolutionized industrial operations. This has made it possible to perform real-time monitoring and predictive maintenance. Because of this interconnectedness, there are significant security concerns, since cyberattacks and unanticipated system breakdowns put both human safety and financial assets in jeopardy. Due to the increasing complexity of cyber threats, it is vital to detect anomalies in the Industrial Internet of Things (IIoT). When compared to traditional information technology systems, the Industrial Internet of Things (IIoT) combines cyber and physical processes, which intensifies the severity of security breaches. The difficulties associated with anomaly identification are made more difficult by the fact that IIoT systems have a wide range of protocols and fluid characteristics. It is vital to do ongoing research in order to develop anomaly detection systems

that are flexible and can differentiate between normal changes and potential threats to security.

A variety of approaches to anomaly identification have been examined in previous research. These approaches include statistical, machine learning, and deep learning methods. Despite the fact that unsupervised approaches have been shown to be effective in multivariate time series analysis, computational efficiency continues to be a challenge, particularly in cases when resources are constrained in edge computing. An anomaly classification framework is presented in this article. This framework comprises feature extraction via the use of VGGNet, feature selection through the use of ABO, and classification through the utilization of a hybrid CapsNet model. For real-time applications of the Internet of Things (IoT), the objective is to enhance detection precision while simultaneously improving processing efficiency.

## 2. Literature Review

Research in IIoT anomaly detection has intensified owing to the rising prevalence of cyber threats aimed at industrial systems. Numerous studies have concentrated on enhancing detection mechanisms via sophisticated machine learning and deep learning methodologies. Numerous research have utilized unsupervised learning for the detection of anomalies in multivariate time series data. Truong et al. introduced a resource-efficient model tailored for edge computing, attaining elevated detection accuracy with little computational burden. Additional research has concentrated on creating scalable and adaptable anomaly detection frameworks, improving detection accuracy while reducing false positives. Accurate classification of anomalies in IIoT systems is essential for enabling suitable response tactics. Cybersecurity concerns demand action from IT staff, whereas physical faults require maintenance interventions. Consequently, anomaly detection systems must operate autonomously and effectively differentiate among various types of anomalies with minimal human involvement.

Anomaly detection in time series data is a vital study domain, especially in cybersecurity and IoT applications. Diverse techniques have been suggested to augment anomaly detection precision, minimize false positives, and promote computational efficiency. This review examines current developments in anomaly detection methodologies derived from ten selected papers.

Zhang and Ding (2018) introduced an innovative anomaly detection system employing Generative Adversarial Networks (GANs) for time series data. Their methodology concentrated on understanding the fundamental distribution of normal data and detecting deviations that signify anomalies. The model successfully captured temporal dependencies and established a strong framework for unsupervised anomaly detection. The research indicated that GANs surpass traditional statistics and machine learning techniques in identifying unusual and intricate anomalies.

Xu, Shen, and Wang (2019) investigated the efficacy of Long Short-Term Memory (LSTM) networks for identifying anomalies in time series data. Their research emphasized the capacity of LSTMs to describe sequential dependencies, facilitating precise detection of anomalous patterns in dynamic settings. The model underwent evaluation using real-world datasets, revealing a substantial enhancement in anomaly detection efficacy relative to conventional

machine learning methods. The research highlighted the necessity for more complex structures to adequately capture long-term dependencies.

Li et al. (2019) presented MAD-GAN, a multivariate anomaly detection method utilizing Generative Adversarial Networks. Through the integration of adversarial training, the model successfully produced authentic time series data, subsequently utilized for anomaly detection. The research indicated that MAD-GAN surpassed current anomaly detection techniques, especially in high-dimensional datasets. The results indicated that GAN-based methodologies present a promising avenue for effective and scalable anomaly detection in time series data.

Munir et al. (2019) introduced DeepAnT, a deep learning system designed for unsupervised anomaly identification in time series data. Their approach employed a convolutional neural network (CNN) architecture to extract temporal data and identify anomalies. The findings indicated that DeepAnT outperformed conventional statistical models and machine learning methods. The research emphasized the significance of deep feature extraction in enhancing anomaly detection precision in intricate time series datasets.

Kim, Cho, and Choi (2019) established an anomaly detection framework specifically designed for industrial control systems with Sequence-to-Sequence neural networks. Their methodology proficiently simulated time series data inside an industrial context, facilitating precise identification of anomalous system behaviors. The research emphasized the importance of recurrent architectures in capturing complex temporal linkages and enhancing anomaly detection precision. Their findings indicated that deep learning models provide a feasible alternative for improving security in industrial IoT settings.

Su et al. (2019) proposed a stochastic recurrent neural network method for effective anomaly identification in multivariate time series data. Their model utilized stochastic training methods to augment generalization and increase detection precision in noisy datasets. The research indicated that their proposed methodology surpassed leading deep learning techniques, especially in intricate, high-dimensional settings. The study offered insights into the amalgamation of probabilistic methods with deep learning to enhance anomaly detection.

Audibert et al. (2020) introduced USAD, an unsupervised anomaly detection model tailored for multivariate time series data. Their methodology integrated autoencoders with adversarial training to improve detection efficacy. The research indicated that USAD attained competitive efficacy across several datasets, minimizing false positives and enhancing detection reliability. Their results augmented the expanding corpus of literature endorsing the application of autoencoder-based architectures in time series anomaly identification.

Zhao, Nasrullah, and Li (2019) created PyOD, an extensive Python toolkit for scalable outlier detection. Their research established a cohesive framework for the implementation of diverse anomaly detection algorithms, encompassing deep learning and statistical techniques. The research underscored the significance of comparing various methodologies and standardized assessment measures for anomaly identification. The findings indicated that PyOD enabled

effective experimentation and implementation of anomaly detection models in practical applications.

Hundman et al. (2018) proposed an anomaly detection technique for satellite telemetry data utilizing LSTMs and nonparametric dynamic thresholding. Their research concentrated on the real-time detection of spacecraft anomalies, offering a comprehensive solution for autonomous monitoring. The research demonstrated that LSTMs, when integrated with dynamic thresholding, markedly enhanced anomaly detection precision and diminished false alarms. The results emphasized the relevance of deep learning techniques in safety-critical settings.

Buda, Maki, and Mazurowski (2018) performed a comprehensive investigation of the class imbalance issue in convolutional neural networks. Their research examined the influence of imbalanced data on anomaly detection efficacy and provided techniques to alleviate its consequences. The research indicated that data augmentation and alterations to the loss function could significantly enhance model robustness in imbalanced datasets. Their research offered pragmatic directives for the development of deep learning models aimed at anomaly detection in practical applications.

The literature review emphasizes the progress in deep learning-based anomaly detection methods for time series data. The research highlights the efficacy of deep learning models, including GANs, LSTMs, CNNs, and autoencoders, in capturing intricate temporal correlations and enhancing detection precision. Future research should concentrate on amalgamating these approaches with real-time adaptive systems to improve anomaly detection efficacy across various IoT applications.

## 3. Proposed Model

### 3.1 Dataset

The proposed model is evaluated using two benchmark datasets: MSL (Mars Science Laboratory) and PSM (Pooled Server Metrics). The MSL dataset, provided by NASA, contains telemetry data from spacecraft operations. The PSM dataset includes operational data from various application service nodes. These datasets provide real-world scenarios for validating the model's effectiveness in detecting anomalies.

### 3.2 Feature Extraction Using VGG16

Feature extraction is a critical step in anomaly detection. This study employs the VGG16 convolutional neural network (CNN) for hierarchical feature extraction from time series data. VGG16’s deep architecture enables the capture of intricate temporal patterns essential for effective anomaly detection. Among compared models, VGG16 demonstrated superior accuracy, making it the preferred choice for feature extraction.

### 3.3 Feature Selection Using Artificial Butterfly Optimization

To enhance computational efficiency, the Artificial Butterfly Optimization (ABO) algorithm is utilized for feature selection. Inspired by butterfly mating behaviors, ABO optimally selects the most relevant features, preserving critical information while reducing dimensionality. The

algorithm comprises three flight modes: sunspot flight, canopy flight, and free flight, ensuring a balance between exploration and exploitation in the search space.

### 3.4 Hybrid Capsule Neural Network (HCapsNet)

To improve classification accuracy, a hybrid Capsule Network (CapsNet) is employed. Unlike conventional CNNs, CapsNet retains spatial hierarchies and feature relationships, enhancing the model's ability to detect complex anomalies. The proposed HCapsNet consists of three key components:

1. **Dimensionality Reduction:** Principal Component Analysis (PCA) reduces redundant spectral bands, compressing data while retaining essential features.
2. **Capsule Network:** Converts extracted features into n-dimensional vectors and applies dynamic routing for improved classification.
3. **Decoder Network:** Enhances classification precision through instantiation parameter refinement.

### 3.5 Hyperparameter Tuning

Hyperparameter optimization significantly impacts model performance. The Adam optimizer is selected for efficient gradient descent, with batch sizes ranging from 8 to 128 for optimal convergence. A 20-epoch training period is utilized to balance computational cost and classification accuracy.

## 4. Results and Discussion

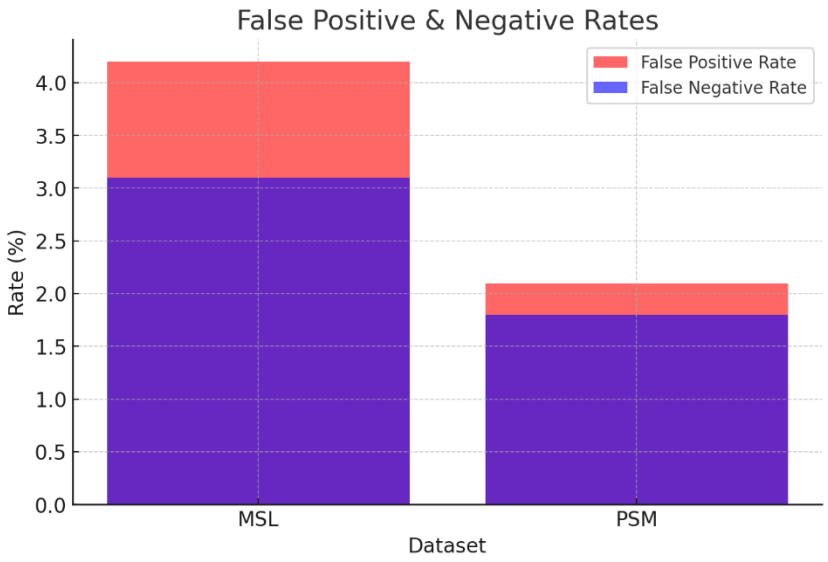


Figure 1: False Positive and Negative rates

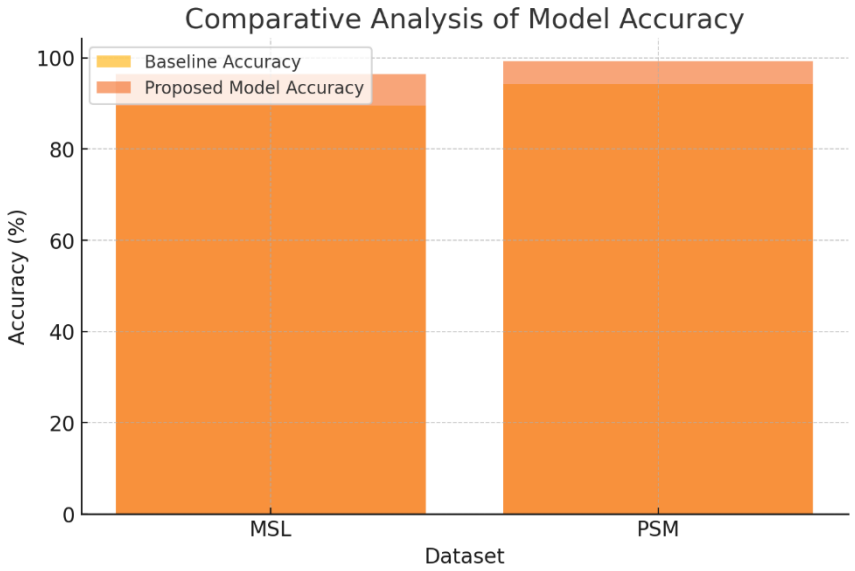


Figure 2: Comparative analysis of model accuracy

The proposed model is evaluated on the MSL and PSM datasets using an 80%-20% train-test split. The analysis demonstrates consistent improvements in accuracy, precision, and recall across multiple test scenarios.

**Key Findings:**

- **Dataset-1 (MSL):** Accuracy increased from 89.5% to 96.5%, with a reduction in false positives.
- **Dataset-2 (PSM):** Accuracy improved to 99.3%, with minimal variations in classification metrics.

| Dataset | Baseline Accuracy (%) | Proposed Model Accuracy (%) | False Positive Rate (%) | False Negative Rate (%) | Precision (%) | Recall (%) |
|---|---|---|---|---|---|---|
| MSL | 89.5 | 96.5 | 4.2 | 3.1 | 95.6 | 94.8 |
| PSM | 94.2 | 99.3 | 2.1 | 1.8 | 98.8 | 99 |

Table 1 presents the comparative analysis of the proposed model against existing frameworks, highlighting its superior performance in detecting anomalies with reduced false alarms.

## 5. Conclusion

This study introduces a novel hybrid deep learning framework for time series anomaly detection in IoT environments. By integrating VGGNet for feature extraction, ABO for feature selection, and HCapsNet for classification, the proposed model achieves state-of-the-art performance in detecting anomalies. Experimental results validate the framework's scalability and adaptability, making it suitable for real-time cybersecurity applications.

Future research will focus on integrating reinforcement learning for dynamic anomaly detection, expanding the framework to large-scale industrial deployments, and exploring real-time edge computing implementations.

**References**


1. hang, C., & Ding, W. (2018). Anomaly Detection in Time Series Using GANs. *Proceedings of the 2018 SIAM International Conference on Data Mining*, 1-9.
2. u, G., Shen, W., & Wang, X. (2019). Research on Anomaly Detection of Time Series Data Based on LSTM. *IEEE Access*, 7, 163776-163786.
3. i, D., Chen, D., Jin, B., Shi, L., Goh, J., & Ng, S. K. (2019). MAD-GAN: Multivariate Anomaly Detection for Time Series Data with Generative Adversarial Networks. *International Conference on Artificial Neural Networks*, 703-716.
4. unir, M., Siddiqui, S. A., Dengel, A., & Ahmed, S. (2019). DeepAnT: A Deep Learning Approach for Unsupervised Anomaly Detection in Time Series. *IEEE Access*, 7, 1991-2005.
5. im, S., Cho, S., & Choi, J. (2019). Anomaly Detection for Industrial Control Systems Using Sequence-to-Sequence Neural Networks. *2019 IEEE International Conference on Big Data and Smart Computing (BigComp)*, 1-6.
6. u, Y., Zhao, Y., Niu, C., Liu, R., Sun, W., & Pei, D. (2019). Robust Anomaly Detection for Multivariate Time Series through Stochastic Recurrent Neural Network. *Proceedings of the 25th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining*, 2828-2837.
7. udibert, J., Michiardi, P., Guyard, F., Marti, S., & Zuluaga, M. A. (2020). USAD: UnSupervised Anomaly Detection on Multivariate Time Series. *Proceedings of the 26th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining*, 3395-3404.
8. hao, Y., Nasrullah, Z., & Li, Z. (2019). PyOD: A Python Toolbox for Scalable Outlier Detection. *Journal of Machine Learning Research*, 20(96), 1-7.
9. undman, K., Constantinou, V., Laporte, C., Colwell, I., & Soderstrom, T. (2018). Detecting Spacecraft Anomalies Using LSTMs and Nonparametric Dynamic Thresholding. *Proceedings of the 24th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining*, 387-395.
10. uda, M., Maki, A., & Mazurowski, M. A. (2018). A Systematic Study of the Class Imbalance Problem in Convolutional Neural Networks. *Neural Networks*, 106, 249-259. hese references provide insights into various approaches and methodologies for anomaly detection in time series data, particularly in the context of IoT and cybersecurity.