Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN: 2581 - 611X)
VOLUME:9, ISSUE:1, JANUARY 2026, PAPER NUMBER:8

LAFA : An AI Driven Anomaly Detection Framework in 6G-Enabled Industry 4.0

Vishnu Prasad D [1], Saraswathi S [2]

Research Scholar[1], Professor[2]
Dept. of Information Technology,
Puducherry Technological University, Puducherry, India.
vishnuprasad@ptuniv.edu.in, s.saraswathy@ptuniv.edu.in

Abstract: *Real-time anomaly detection becomes more difficult as Industrial Internet of Things (IIoT) devices proliferate because of the high-dimensional, dynamic, and massive data streams they generate. It takes accurate, scalable, and effective approaches to handle these complexities. This study introduces the League-Based Adaptive Foraging Algorithm (LAFA), a two-phase framework that combines the League Championship Algorithm (LCA) with the Honey Badger Algorithm (HBA). Through competitive model selection, LCA improves accuracy, and HBA adjusts detection settings to balance exploitation and exploration for accurate anomaly identification. LAFA performs better than traditional techniques when tested on real-world datasets, exhibiting greater scalability, accuracy, and adaptability. Because it can handle changing Industry 4.0 data, it works especially well in intricate industrial settings. In addition to its technical advantages, LAFA guarantees system security, operational effectiveness, and dependability. It advances Industry 4.0 technology by tackling important anomaly detection issues and establishing the groundwork for broad industrial deployment.*

Keywords: *6G Technology, Industry 4.0, IIoT, Anomaly Detection, LAFA, LCA, HBA.*

1. INTRODUCTION:

A. Challenges in Real-Time Anomaly Detection

Significant difficulties in real-time anomaly detection have developed with the introduction of 6G-enabled IIoT. The huge volume of data produced by networked devices presents such challenges since it must to be processed and examined instantly in order to spot differences which could be signs of abnormalities. This data's high dimensionality, which includes a variety of factors like temperature, vibration, and network activity, makes detection a challenge. Also while industrial conditions are dynamic and non-linear, systems should be able to react quickly to changing conditions.

Scalability is another critical issue. As IIoT networks grow, they incorporate more devices, sensors, and communication nodes, leading to an exponential increase in data volume. Traditional anomaly detection methods, which are usually designed for smaller and simpler datasets, cannot handle the processing needs. Additionally, the presence of noise and inconsistencies in raw data further complicates anomaly detection, often leading to false positives or missed detections. Latency is a pressing concern in real-time systems. Delays in data transmission, processing, or analysis can result in critical failures, such as machine breakdowns or cybersecurity breaches. Existing systems relying on centralized architectures face limitations due to bandwidth constraints and processing delays, making them unsuitable for real-time industrial applications.

Finally, the multidimensional nature of IIoT data adds another layer of complexity. Many anomalies involve interactions between multiple parameters, which are complicated to figure out using traditional univariate methods. To address these challenges, a paradigm shift is needed, leveraging advanced technologies like 6G networks, decentralized architectures, and intelligent algorithms capable of processing vast, complex datasets in real-time.

B. Contributions of 6G Technology to Anomaly Detection

The transition to 6G networks brings unprecedented advancements in the field of anomaly detection for Industry 4.0. The ultra-low latency of 6G enables real-time detection of anomalies, a critical factor in environments where rapid response is essential to prevent disruptions. This feature can be particularly crucial for applications like predictive maintenance, where expensive downtime can occur from a delay in finding equipment defects.

Massive connectivity is another transformative feature of 6G. Unlike its predecessors, 6G can support millions of devices per square kilometer, facilitating the seamless integration of IIoT devices across vast industrial networks. This level of connectivity allows comprehensive monitoring and data collection, providing a holistic view of industrial operations and enabling more accurate anomaly detection.

High data transmission rates further enhance the ability to process complex datasets in real-time. The speed at which data can be transmitted to and from centralized or edge processing units ensures minimal delays, even when handling large volumes of data. This capability is particularly advantageous in scenarios where anomalies evolve rapidly, such as cybersecurity threats or sudden equipment malfunctions. Decentralized processing is additionally made easier as a result of 6G's support for edge computing, which lessens the need for central servers.

By processing data closer to the source, edge computing minimizes latency and bandwidth usage, ensuring faster anomaly detection and response times. These advancements make 6G an enabler for next-generation anomaly detection frameworks, addressing the limitations of traditional systems and paving the way for innovative approaches like the LAFA framework.

C. Traditional Anomaly Detection Techniques and Their Limitations

While essential in identifying departures from typical behavior, classic anomaly detection methods have serious drawbacks when applied to the high-dimensional, dynamic datasets of 6G-enabled IIoT environments. Z-score analysis and moving averages are statistical methods that use historical data to identify anomalies. Notwithstanding their computational effectiveness, these methods have challenges focused on abnormalities that include several variables or non-linear patterns. Supervised and unsupervised models are two variations on neural network (ML) approaches offering sophisticated anomaly detection capabilities.

Labeled datasets are necessary for training supervised models such as support vector machines (SVM) and decision trees, but they are either expensive or unavailable in industrial contexts. However, when applied to noisy or sparse information, unsupervised techniques like isolation forests and k-means clustering may result in significant false-positive rates even while these methods are effective in detecting unknown anomalies.

Convolutional neural networks (CNNs) and autoencoders are two examples of deep learning models that are excellent at processing high-dimensional input. However, in real-time IIoT systems, their training necessitates big labeled datasets and substantial computational resources, which are not always possible. In addition, these models frequently lack explainability, which makes it challenging for stakeholders to understand their choices.

Scalability represents another significant constraint. Conventional methods are frequently made for smaller datasets, and when data volume and complexity rise, they perform worse. Many older systems' centralized architecture contributes to latency problems, rendering them inappropriate for the rapid demands of IIoT systems enabled by 6G. Innovative frameworks like LAFA, which are built for scalability, adaptability, and real-time performance, are necessary for overcoming these constraints.

D. Overview of the LAFA Framework

An innovative method for anomaly detection created especially to meet the demands of Industry 4.0 settings provided by 6G is the League-Based Adaptive Foraging Algorithm (LAFA). LAFA combines the League Championship Algorithm (LCA) and Honey Badger Algorithm (HBA), two sophisticated algorithms, into a cohesive two-phase structure.

LCA encourages machine learning models to refine themselves competitively in the initial stage. LCA puts models into teams so they may compete with one another in identifying anomalies, a concept inspired by sports leagues. Only the most precise and effective models are chosen for the following phase thanks to this iterative procedure. Models like as PCA, Isolation Forest, and autoencoders are frequently used, utilizing their distinct advantages to detect various kinds of abnormalities. The best-performing models' detection parameters are dynamically adjusted by HBA in the second step. HBA alternates between investigating novel solutions and taking advantage of promising regions of the dataset, mimicking the foraging behavior of honey badgers. By improving anomaly detection's accuracy and resilience, this adaptive method enables the ability to detect subtle or uncommon anomalies.

2. RELATED WORKS

Anomaly detection in Industrial Internet of Things (IIoT) systems has garnered significant attention due to the increasing reliance on interconnected devices in industrial applications. The need to maintain robust, secure, and efficient operations in the face of various operational and security anomalies has driven research into advanced techniques, including machine learning (ML), deep learning (DL), and hybrid models. The following presents a review of several notable contributions to anomaly detection in IIoT systems.

One of the innovative approaches in anomaly detection for IIoT systems involves the use of reinforcement learning combined with GANs. Benaddi et al. (2022) propose a novel anomaly detection framework for industrial IoT based on distributional reinforcement learning and GANs. Their study emphasizes the application of generative models to simulate normal data distributions, allowing for the detection of deviations that signify potential system anomalies. This approach is particularly advantageous in detecting subtle or rare anomalies that traditional methods may overlook.

In another significant contribution, Cai et al. (2022) present CapBad, a content-agnostic anomaly detection system for industrial control protocols. This system focuses on analyzing the payloads of communication packets rather than the content itself. By leveraging the unique features of industrial control protocols, CapBad is capable of identifying abnormalities that would otherwise go unnoticed by conventional network anomaly detection methods. This content-agnostic approach allows for broader application across diverse industrial settings.

The increasing complexity of IoT networks and sensor data has led to an abundance of AI-driven anomaly detection techniques. DeMedeiros et al. (2023) conducted a comprehensive survey on AI-based anomaly detection in IoT and sensor networks, identifying key trends and challenges in the field.

Their work highlights the importance of utilizing machine learning models, such as clustering and classification algorithms, to effectively identify anomalous patterns in multivariate time-series data. They also discuss the integration of deep learning techniques to enhance the accuracy and scalability of anomaly detection systems in large-scale industrial settings.

Feng et al. (2022) introduced a deep learning-based approach to anomaly detection in IIoT systems using a graph autoencoder model. Their method, which focuses on one-class anomaly detection, is designed to detect anomalies in systems where labeled data is scarce. The proposed model integrates graph-based representations with autoencoders, enabling it to capture complex relationships within IIoT data and detect previously unseen anomalies. This approach is especially useful in applications where only a limited set of normal data is available for training.

Gyamfi and Jurcut (2023) propose a hybrid model combining OI-SVDD (Online Incremental Support Vector Data Description) and AS-ELM (Adaboost with Extreme Learning Machine) for online network intrusion detection in IIoT. Their method is specifically designed for real-time applications, enabling it to detect cyberattacks on IIoT networks as they occur. The hybrid model's capability to handle both intrusion detection and anomaly classification makes it particularly effective for protecting critical industrial infrastructure from evolving threats.

Karadayi et al. (2020) present a hybrid deep learning framework for unsupervised anomaly detection in multivariate spatio-temporal data. This method is particularly suitable for IIoT systems where time-series data is collected from multiple sensors over time. By integrating deep learning methods with a robust unsupervised learning approach, the framework is able to detect both spatial and temporal anomalies, which is crucial for identifying faults or malfunctions in complex industrial systems.

Khan et al. (2022) focus on an explainable deep learning framework for cyber threat detection in industrial IoT networks. Their work highlights the importance of interpretability in AI models used for cybersecurity. The explainability of deep learning models allows operators to understand and act on the insights generated by the system. This feature is critical in industrial applications, where decisions need to be justified and risks minimized. The framework proposed by Khan et al. utilizes deep learning techniques to detect cyber threats while ensuring that the decision-making process is transparent and understandable.

Kong et al. (2023) explore the integration of generative models with bidirectional LSTM (Long Short-Term Memory) and attention mechanisms for anomaly detection in industrial systems. Their approach focuses on leveraging sequential data and attention mechanisms to improve the detection of anomalies in time-series data, a common characteristic of IIoT environments. The bidirectional LSTM allows the model to capture both past and future context, which is essential for accurate anomaly detection in dynamic industrial processes.

Maggipinto et al. (2022) present a deep convolutional autoencoder-based approach for anomaly detection in industrial systems, specifically targeting non-image, two-dimensional data. This method is particularly useful in semiconductor manufacturing, where data generated is typically non-image and includes sensor readings and performance metrics. Even without image-based data, the authors' method successfully detects abnormalities in industrial processes by utilizing convolutional layers in an autoencoder architecture

Mofidul et al. (2022) address the challenge of real-time anomaly detection in energy data within industrial IoT infrastructures. Their research focuses on integrating edge and cloud AI to provide a secure and robust monitoring system for energy consumption. The system is designed to detect anomalies related to energy usage, which can indicate issues such as equipment failure or inefficiencies. In order to offer the finest energy management in industrial settings, this real-time monitoring system is essential.

In IIoT contexts, Nizam et al. (2022) concentrate on deep anomaly detection frameworks for multivariate time-series data. Deep learning techniques are used in their suggested framework to detect anomalies in real-time, which is crucial for sectors that depend on ongoing system data monitoring. For industrial processes to run smoothly and to avoid system outages, the ability to identify irregularities in time-series data is essential. With a variety of strategies utilizing machine learning, deep learning, and hybrid models to handle the intricacies of industrial contexts, anomaly detection research for IIoT has advanced significantly in recent years.

From GAN-based models to hybrid frameworks that include extreme learning machines and support vector machines, these research demonstrate the variety of methods being investigated to improve the security, effectiveness, and dependability of IIoT systems. Future studies will probably keep improving these techniques and incorporate them into scalable, real-time industrial applications. Every one of these studies advances the creation of more reliable and precise anomaly detection systems, guaranteeing the security and effectiveness of IIoT systems as companies continue to embrace increasingly automated and networked technology.

3. PROPOSED WORKS

A. Data Collection and Preprocessing

The initial stage in anomaly detection for IIoT systems is data collection and preparation. High-dimensional data is continuously streamed by IIoT devices from a variety of sources, including sensors, actuators, and controllers. Since this data is usually unstructured, noisy, and inconsistent, pretreatment procedures are crucial to getting it ready for efficient anomaly identification.

Data Collection

The primary datasets used for training and evaluation in this study include:

1. SECOM Manufacturing Dataset: This dataset includes sensor data from a semiconductor manufacturing process, with the goal of detecting anomalies in the production process.
2. NASA's CMAPSS Dataset: With an emphasis on identifying malfunctions and other irregularities, this dataset includes time-series sensor data from aircraft engines.

Data Preprocessing Steps

The preprocessing steps aim to clean and normalize the data to ensure the model can detect anomalies accurately. The steps include:
1. Normalization: Given the high-dimensional nature of IIoT data, normalization is applied to scale all features to a common range (usually between 0 and 1). This step prevents features with larger scales from dominating the anomaly detection process.

2. Handling Missing Values: To make sure the dataset is complete and prepared for training, missing values are imputed using methods like mean imputation or interpolation.
3. Outlier Removal: Outliers that could obstruct model learning are found and eliminated using statistical techniques. This is crucial since outliers are frequently mistakes in data collecting instead of true oddities.
4. Feature Selection: Recursive Feature Elimination (RFE) and Principal Component Analysis (PCA) are two feature selection techniques that reduce overfitting and improve model performance by reducing the number of unnecessary features.
5. For the purpose of evaluating the model, the preprocessed data is divided into training and test datasets.

League Championship Algorithm (LCA)

The League Championship Algorithm (LCA) is an iterative optimization method designed to refine machine learning models for anomaly detection. LCA works by simulating a competitive environment where different models compete to improve their performance over time. Iteratively improving the performance of models like autoencoders, isolation forests, and principal component analysis (PCA) is the aim.

LCA Process Overview

1. LCA models the competition between different anomaly detection techniques as a "league." The competition occurs in several rounds:
2. **Initialization:** The algorithm starts with a set of machine learning models, such as PCA, Isolation Forest, and Autoencoders. These models are trained on the preprocessed dataset.
3. **Competition:** During each round, the models "compete" by predicting anomalies in the dataset. The predictions are evaluated based on performance metrics (accuracy, recall, precision, etc.), and the models that perform poorly are penalized.
4. **Refinement:** The models that perform better are retained and further refined in subsequent rounds. The process continues iteratively, with models adjusting their parameters based on feedback to improve their anomaly detection capabilities.
5. **Final Selection:** After several rounds, the models with the best performance are selected, and their parameters are fine-tuned to produce the final anomaly detection model.

Model Competition and Evaluation

1. To evaluate the performance of each model, we use the following metrics:
2. Accuracy: The proportion of correctly classified instances (both anomalies and normal instances).
3. **Recall**: The proportion of actual anomalies correctly identified by the model.
4. **Precision**: The proportion of predicted anomalies that are true anomalies.
5. **F1-Score**: Precision and recall are balanced using the harmonic mean of the two measurements.
6. Finding the best model for identifying abnormalities in IIoT environments is aided by the competition between models.

C. Honey Badger Algorithm (HBA)

After the competition stage in the League Championship Algorithm, the Honey Badger Algorithm (HBA) is applied to further refine the results. HBA is a nature-inspired optimization algorithm that adapts dynamically to enhance the accuracy of anomaly detection.

HBA Overview

1. The Honey Badger Algorithm is a hybrid algorithm that combines the exploration and exploitation phases of optimization. It adapts detection parameters based on the current state of the anomaly detection task, helping to refine the model's performance.
2. **Exploration**: In the initial phase, HBA explores different parameter configurations and model variations, searching for the optimal settings.
3. **Exploitation**: In the later stages, HBA focuses on exploiting the best-performing configurations to further fine-tune the model and enhance its detection accuracy.
4. HBA dynamically adapts the search for optimal parameters, ensuring the model remains robust against varying data patterns and anomalies. It does so by adjusting detection thresholds, selecting optimal features, and fine-tuning hyperparameters.

HBA's Contribution

HBA enhances the results from LCA by introducing an adaptive search process. This dynamic adjustment of parameters allows for a more precise detection of anomalies, making the model more effective in real-world IIoT systems, where data can change over time.

4. LAFA ARCHITECTURE

The architecture illustrates a multi-stage anomaly detection pipeline for Industrial IoT (IIoT) systems, combining competitive machine learning selection with automated optimization. The process begins with the ingestion of raw IIoT data, which undergoes preprocessing to prepare it for model training and evaluation. In the first stage, the League Championship Algorithm (LCA) initiates a model competition among four unsupervised or deep learning anomaly detection techniques—PCA, LOF, Isolation Forest, and Autoencoders. The LCA compares model performance and selects the best performing candidate, which becomes the initial champion model with default parameters.

After champion selection, the system generates an initial visualization and summary report to show how the chosen model behaves on the dataset. The next step involves model refinement through the Honey Badger Algorithm (HBA). The champion model from LCA is fed into HBA, which performs automated hyperparameter tuning across 50 iterations. During this search, HBA optimizes the model using the F1 score as the primary fitness function, identifying the best configuration that balances detection precision and sensitivity.

Once the optimal F1 value is determined, it feeds back into a second round of the LCA, now executed using the refined metrics gained from HBA. This ensures that the competition is re-evaluated with updated parameters, validating whether the selected model remains superior or whether another model outperforms under optimized settings. A final visualization and performance report is generated to provide comprehensive insight into detection quality.

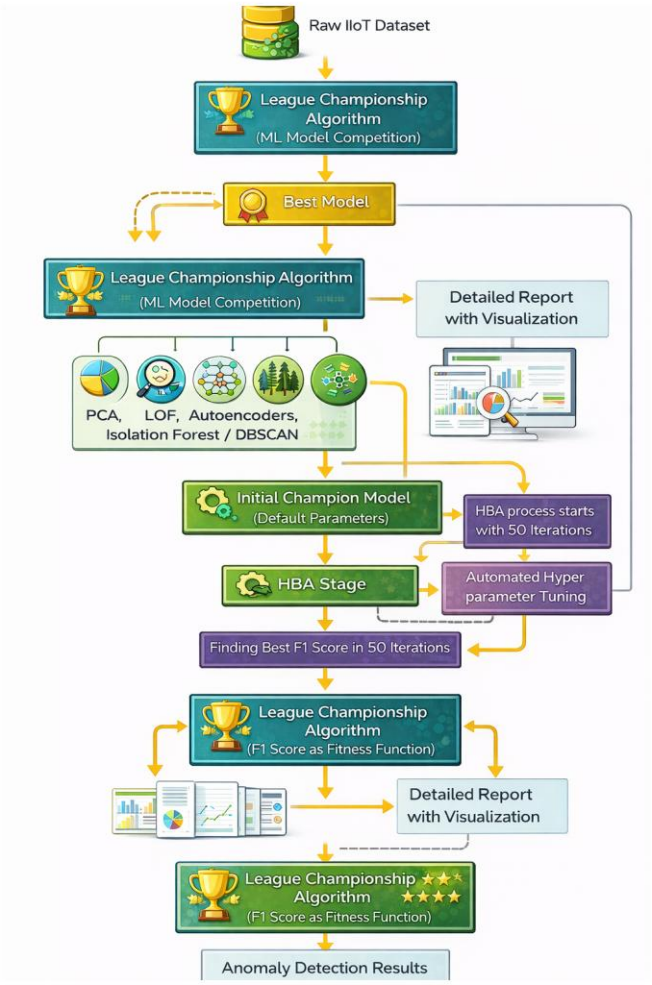

Fig. 1. LAFA ARCHITECTURE

5. ALGORITHM

Stage 1: Anomaly Detection Using LCA (League Championship Algorithm)
In this stage, multiple competing machine learning models are used to detect anomalies in the IIoT dataset. The models compete in a way similar to sports leagues, where each model (team) is evaluated based on its anomaly detection performance.

Anomaly Detection by Each Model: Each competing model (PCA, LOF, Autoencoders, Isolation Forest, DBSCAN) is applied to the dataset $X = \{x_1, x_{2,\ldots\ldots} x_n\}$ and anomalies are identified based on the specific model's characteristics.
PCA: Dimensionality reduction by computing eigenvectors and eigenvalues of the covariance matrix C of the dataset:

$$c = \frac{1}{n}\sum_{i=n}^{n}(x_i - u)(x_i - \mu)^T$$

Anomalies are identified by projecting data into a lower-dimensional space and checking for data points that deviate significantly.

LOF: Local outlier factor score based on local density:

$$LOF(p) = \frac{\Sigma_0 \in N_k(p) \frac{LRD^{(0)}}{LRD(P)}}{|N_k(p)|}$$

Where LRD(p)LRD(p)LRD(p) is the local reachability density for a point p.

Autoencoders: The reconstruction error is computed as:

$$L(x, \hat{x}) = \|x - \hat{x}\|^2$$

Anomalies are detected if the reconstruction error $L(x, \hat{x})$ exceeds a threshold.

Isolation Forest: The anomaly score for a point xxx is computed based on the path length required to isolate x:

$$Anomaly\ score(x) = 2^{-\frac{h(x)}{c(n)}}$$

Where $h(x)$ is the path length for point x, and $c(n)$ is the average path length for a random tree.

DBSCAN: Points that do not belong to any dense region (clusters) are classified as anomalies.

Selection of Best Models: Each model's performance is evaluated, and the best-performing models (based on metrics like detection accuracy or precision) are selected to move forward in the process.

Stage 2: Model Enhancement Using HBA (Honey Badger Algorithm)

Once the best models are selected in Stage 1, the HBA algorithm refines them by alternating between exploration and exploitation.

1. **Exploration and Exploitation**: The HBA algorithm explores different regions of the dataset and exploits promising areas to fine-tune the model parameters for anomaly detection. This can be modeled as an optimization problem:

$$Maximize\ L = \sum_{i=1}^{n} Loss(x_i, \hat{x}_i)$$

Where $Loss(x_i, \hat{x}_i)$ is the error in the reconstruction or detection of the anomaly for each point $x_i and\ \hat{x}_i$ is the predicted or reconstructed value for that point.

2. **Adaptive Refinement**: In the HBA, exploration increases diversity in the search space, while exploitation focuses on the most promising regions:

$$Exploration: \quad \mu_{explore} = \frac{1}{|S^{explore}|} \sum_{x_i \epsilon S^{explore}} loss(x_i, \hat{x}_i)$$

$$Exploitation: \quad \mu_{exploit} = \frac{1}{|S^{exploit}|} \sum_{x_i \epsilon S^{exploit}} loss(x_i, \hat{x}_i)$$

The refinement is continuously improved by focusing on areas with the highest anomaly detection errors.

Final Anomaly Detection and Categorization

After refining the models using HBA, the final anomaly detection step identifies the anomalies based on the fine-tuned model. The detected anomalies are categorized based on their type, such as:

- **Cybersecurity Threats**
- **Operational Failures**
- **Sensor Data Anomalies**
- **Process Deviations**

Mathematically, anomalies are classified by comparing the model's predictions to known anomaly categories and thresholds. If the model identifies a deviation beyond an acceptable threshold, it is classified into the relevant category.

$$Categorization : Category(x) = ArgMax(L_i)$$

Where L_i is the likelihood score for category iii, and the highest score determines the anomaly's category.

Alerts and Reports / Industrial System Response

Based on the categorization, alerts are generated for the identified anomalies, and the system is prepared to respond accordingly (e.g., initiate a security protocol, alert maintenance teams, or adapt operational procedures).

This approach ensures dynamic anomaly detection and categorization while handling complex, multidimensional data in Industry 4.0 environments.

6. COMPARISON BETWEEN LAFA & EXISTING SYTEMS

Aspect	Existing Anomaly Detection Techniques	LAFA (League-Based Adaptive Foraging Algorithm)
Detection of Complex Anomalies	Struggles with multi-dimensional, subtle, or complex anomalies.	Capable of handling complex, multi-dimensional, and subtle anomalies due to iterative model competition and refinement.
Scalability	Often struggles with scalability in large datasets, especially for high-dimensional data (e.g., LOF and Autoencoders).	Highly scalable, as it dynamically adapts to different data volumes and structures, handling large and high-dimensional datasets effectively.
Model Adaptability	Some techniques (like PCA) are rigid and not adaptable to changing data patterns, while others (e.g., Autoencoders) need frequent retraining.	LAFA adapts to evolving data by refining the best models selected during the LCA phase, making it highly adaptable to new, unseen anomalies.

Computational Efficiency	Computationally expensive in some cases, especially with LOF, Autoencoders, and k-NN-based methods.	Computationally efficient, thanks to the isolation process in LCA and the optimization in HBA, reducing training time and resource consumption.
Multi-Dimensional Data Handling	Limited in handling high-dimensional data (e.g., PCA assumes linearity, LOF can be computationally expensive for high dimensions).	Excellent for multi-dimensional data, utilizing competition (LCA) and dynamic refinement (HBA) to identify anomalies in complex, high-dimensional spaces.
Noise Sensitivity	Highly sensitive to noise (e.g., PCA, LOF) or requires heavy preprocessing.	LAFA is robust to noise due to its multi-stage approach, which isolates and refines models iteratively, making it more resilient to noisy data.
Anomaly Detection Speed	May suffer from delays in real-time detection, especially in complex models like Autoencoders and LOF.	Real-time anomaly detection is achieved through the combination of ultra-low latency 6G and the efficient model selection and refinement process.
Model Accuracy	High accuracy in some cases (e.g., CNN-LSTM in time-series) but may fail on subtle anomalies or complex datasets.	High accuracy and robustness due to the combination of competitive learning (LCA) and adaptive refinement (HBA), effectively detecting both subtle and large-scale anomalies.
Integration with Existing Systems	Requires significant adaptation or retraining to work with new or different datasets (e.g., GANs, CNN-LSTM).	Seamless integration with 6G-enabled IIoT systems, as LAFA is designed to be adaptable and scalable, handling diverse types of datasets and systems.
Real-Time Anomaly Detection	Some methods (like Autoencoders) struggle in real-time, especially on large, streaming data.	LAFA ensures low-latency, real-time detection due to the competition and refinement structure, supported by 6G capabilities.
Detection of Multi-Class Anomalies	May fail to distinguish between different types of anomalies (e.g., cybersecurity vs. operational failure).	Efficiently categorizes and detects multiple anomaly types (cybersecurity, sensor faults, operational failure) by dynamically adjusting the detection model.

7. KEY HIGHLIGHTS OF LAFA OVER EXISTING TECHNIQUES

1. **Adaptability & Scalability**: Large-scale IIoT environments can benefit from LAFA's proficiency with dynamic data and high-dimensional information.
2. **Model Refinement**: The iterative nature of LAFA ensures that models continually improve, which is a significant advantage over static methods like PCA or LOF.
3. **Real-Time Detection**: With 6G technology, LAFA can detect anomalies in real-time, crucial for high-speed, mission-critical industrial applications.
4. **Robustness to Noise**: LAFA's two-stage approach (LCA and HBA) ensures better performance in noisy and high-variance environments compared to other algorithms.

This comparison highlights how LAFA's novel approach to anomaly detection can overcome the limitations of existing methods, offering a more adaptable, scalable, and accurate solution for Industry 4.0 in a 6G-enabled environment

8. EFFECTIVENESS OF HYBRID FRAMEWORK

With an emphasis on data from Industrial Internet of Things (IIoT) devices, the League-Based Adaptive Foraging Algorithm (LAFA) is a powerful hybrid framework created for anomaly detection in 6G-enabled Industry 4.0 environments. The limitations of conventional anomaly detection techniques are addressed by LAFA, which combines the advantages of two optimization algorithms—the League Championship Algorithm (LCA) and the Honey Badger Algorithm (HBA). This results in a reliable, scalable, and adaptable solution that can identify a wide range of anomalies in intricate, multi-dimensional datasets.

Key Components of LAFA

League Championship Algorithm (LCA):

The framework of sports leagues, where several models (representing various machine learning approaches) "compete" for anomaly detection, served as the model's inspiration for LCA. This method uses the same dataset to train and assess several models at once, including PCA, LOF, Autoencoders, Isolation Forest, and DBSCAN. The accuracy of anomaly detection is used to evaluate the models' performances, and the top-performing models advance in the competition. By using the most accurate and effective models in subsequent rounds, this competitive model selection enhances detection performance. By learning from stronger models, LCA also encourages weaker models to continuously improve, which aids in the models' gradual improvement.

Honey Badger Algorithm (HBA):

The best models from LCA are chosen, and then model augmentation is done using HBA. The honey badger's foraging strategy, which alternates between exploration and exploitation to find food, is the basis for HBA. By investigating new parameter spaces and concentrating on regions with encouraging outcomes, HBA improves the chosen models in the context of anomaly detection. While the exploitation phase refines the model to detect tiny anomalies with high precision, the exploration phase enables HBA to find new anomaly patterns. For IIoT systems that produce enormous volumes of data in real time, this combination guarantees that the model continually adapts to complex and dynamic datasets.

9. EFFECTIVENESS IN REAL-WORLD APPLICATIONS

1. Handling Multi-Dimensional and High-Dimensional Data

The capacity of LAFA to manage high-dimensional and multi-dimensional data, which is common in Industry 4.0 applications like IIoT, is one of its key features. Because of their computational complexity or linear assumptions, traditional anomaly detection techniques like PCA and LOF may not work well with high-dimensional data. While the LCA phase makes sure the best models are chosen based on their capacity to handle multi-dimensional spaces, the HBA phase refines the models for better performance, allowing LAFA to effectively detect anomalies in datasets with numerous features.

2. Scalability and Real-Time Detection

In Industry 4.0, real-time anomaly detection is crucial for preventing operational failures, ensuring cybersecurity, and maintaining system efficiency. LAFA's hybrid framework leverages 6G technology's ultra-low latency, massive connectivity, and high data transmission rates, which are critical for real-time anomaly detection. The model selection process in LCA ensures that only the most relevant models are used, reducing computational overhead.

3. Robustness to Noise and Complex Anomalies

IIoT systems frequently deal with complicated abnormalities, sensor errors, and noisy data, which may include minute changes in several dimensions. Complex, multi-dimensional anomalies are difficult to identify using many classic anomaly detection techniques, or they are too sensitive to noise. In order to tackle this issue, LAFA uses two complementing approaches:

- LCA ensures that the models chosen for anomaly detection are robust, as they are selected based on their ability to handle different types of anomalies.
- HBA adapts the models dynamically, allowing them to refine their parameters and focus on detecting rare or subtle anomalies, even in noisy environments. This makes LAFA more resilient to sensor malfunctions and environmental factors that might interfere with other algorithms.

4. Adaptability to Changing Environments

Anomaly detection algorithms must be flexible enough to adapt to the ever-changing sensor networks and operational situations found in IIoT environments. The framework may readily adjust to changing circumstances, such as a shift in sensor behavior, the addition of additional devices, or the development of system procedures, according to LAFA's two-stage method (LCA for model selection and HBA for refining). Compared to traditional methods, which frequently call for manual retraining or fine-tuning to accommodate changes in the data distribution, this flexibility is a major benefit.

5. Flexibility Across Use Cases

The adaptability of LAFA allows it to be used in a wide range of anomaly detection scenarios across Industry 4.0 domains, including manufacturing, healthcare, energy, and transportation. LAFA's competitive selection and dynamic refining make it a suitable solution for a variety of industrial applications, whether the objective is to detect operational problems, cybersecurity risks, or sensor anomalies.

For example:

- In manufacturing, LAFA can detect operational anomalies like machine failures or inefficiencies by analyzing sensor data (temperature, pressure, vibration).
- In healthcare, it can be used to detect anomalies in patient data such as abnormal vitals, identifying potential health risks in real-time.
- In energy, LAFA can identify deviations in power consumption or equipment behavior, ensuring smooth operation and preventing costly outages.

10. CONCLUSION

Given the complexity of Industrial Internet of Things (IIoT) data, an efficient anomaly detection framework is crucial for Industry 4.0. To address current limitations, we introduce the League-Based Adaptive Foraging Algorithm (LAFA), a hybrid approach combining the League Championship Algorithm (LCA) and the Honey Badger Algorithm (HBA). Designed for real-time anomaly detection, LAFA effectively handles high-dimensional, rapidly changing data.LAFA's strength lies in LCA's competitive model selection and HBA's adaptive refinement. LCA ensures that only the best-performing models are retained through an iterative competition process, optimizing detection for complex, high-dimensional anomalies. Meanwhile, HBA enhances robustness by alternating between exploration and exploitation, enabling LAFA to detect subtle irregularities that traditional methods might miss.Utilizing 6G technology, LAFA ensures real-time detection with low latency and high-speed data transmission. Its scalability makes it ideal for Industry 4.0, where datasets are vast and dynamic. Traditional methods struggle with these challenges, but LAFA iteratively refines models, maintaining accuracy while managing computational efficiency.

In conclusion, LAFA integrates advanced algorithms and 6G capabilities to deliver scalable, precise, and adaptive anomaly detection, making it a promising solution for the evolving industrial landscape.-consumption.

11. REFERENCES

[1] Prasad, D Vishnu, and S Saraswathi. "The Role of Anomaly Detection in Industry 4.0: A Survey of Techniques and Applications." Journal of Trends in Computer Science and Smart Technology 6, no. 2 (2024): 125-138. 10.36548/jtcsst.2024.2.003

[2] Benaddi, H ;, M ; Jouhari, K ; Ibrahimi, Othman Ben, Hafsa Benaddi, Mohammed Jouhari, Khalil Ibrahimi, Jalel Ben Othman, and El Mehdi Amhoud. 2022. "Anomaly Detection in Industrial IoT Using Distributional Reinforcement Learning and Generative Adversarial Networks." *Sensors 2022, Vol. 22, Page 8085* 22 (21): 8085. https://doi.org/10.3390/S22218085.

[3] Cai, Jun, Qi Wang, Jianzhen Luo, Yan Liu, and Liping Liao. 2022. "CapBad: Content-Agnostic, Payload-Based Anomaly Detector for Industrial Control Protocols." *IEEE Internet of Things Journal* 9 (14): 12542–54. https://doi.org/10.1109/JIOT.2021.3138534.

[4] DeMedeiros, Kyle, Abdeltawab Hendawi, and Marco Alvarez. 2023. "A Survey of AI-Based Anomaly Detection in IoT and Sensor Networks." *Sensors 2023, Vol. 23, Page 1352* 23 (3): 1352. https://doi.org/10.3390/S23031352.

[5] Feng, Yong, Jinglong Chen, Zijun Liu, Haixin Lv, and Jun Wang. 2022. "Full Graph Autoencoder for One-Class Group Anomaly Detection of IIoT System." *IEEE Internet of Things Journal* 9 (21): 21886–98. https://doi.org/10.1109/JIOT.2022.3181737.

[6] Gyamfi, Eric, and Anca Delia Jurcut. 2023. "Novel Online Network Intrusion Detection System for Industrial IoT Based on OI-SVDD and AS-ELM." *IEEE Internet of Things Journal* 10 (5): 3827–39. https://doi.org/10.1109/JIOT.2022.3172393.

[7] Karadayi, Yildiz, Mehmet N. Aydin, and A. Selçuk Öğ˘renci. 2020. "A Hybrid Deep Learning Framework for Unsupervised Anomaly Detection in Multivariate Spatio-Temporal Data." *Applied Sciences 2020, Vol. 10, Page 5191* 10 (15): 5191. https://doi.org/10.3390/APP10155191.

[8] Khan, Izhar Ahmed, Nour Moustafa, Dechang Pi, Karam M. Sallam, Albert Y. Zomaya, and Bentian Li. 2022. "A New Explainable Deep Learning Framework for Cyber Threat Discovery in Industrial IoT Networks." *IEEE Internet of Things Journal* 9 (13): 11604–13. https://doi.org/10.1109/JIOT.2021.3130156.

[9] Kong, Fanhui, Jianqiang Li, Bin Jiang, Huihui Wang, and Houbing Song. 2023. "Integrated Generative Model for Industrial Anomaly Detection via Bidirectional LSTM and Attention Mechanism." *IEEE Transactions on Industrial Informatics* 19 (1): 541–50. https://doi.org/10.1109/TII.2021.3078192.

[10] Maggipinto, Marco, Alessandro Beghi, and Gian Antonio Susto. 2022. "A Deep Convolutional Autoencoder-Based Approach for Anomaly Detection with Industrial, Non-Images, 2-Dimensional Data: A Semiconductor Manufacturing Case Study." *IEEE Transactions on Automation Science and Engineering* 19 (3): 1477–90. https://doi.org/10.1109/TASE.2022.3141186.

[11] Mofidul, Raihan Bin, Md Morshed Alam, Md Habibur Rahman, and Yeong Min Jang. 2022. "Real-Time Energy Data Acquisition, Anomaly Detection, and Monitoring System: Implementation of a Secured, Robust, and Integrated Global IIoT Infrastructure with Edge and Cloud AI." *Sensors 2022, Vol. 22, Page 8980* 22 (22): 8980. https://doi.org/10.3390/S22228980.

[12] Nizam, Hussain, Samra Zafar, Zefeng Lv, Fan Wang, and Xiaopeng Hu. 2022. "Real-Time Deep Anomaly Detection Framework for Multivariate Time-Series Data in Industrial IoT." *IEEE Sensors Journal* 22 (23): 22836–49. https://doi.org/10.1109/JSEN.2022.3211874.

[13] Qi, Lianyong, Yihong Yang, Xiaokang Zhou, Wajid Rafique, and Jianhua Ma. 2022. “Fast Anomaly Identification Based on Multiaspect Data Streams for Intelligent Intrusion Detection Toward Secure Industry 4.0.” *IEEE Transactions on Industrial Informatics* 18 (9): 6503–11. https://doi.org/10.1109/TII.2021.3139363.

[14] Salam, Abdu, Faizan Ullah, Farhan Amin, and Mohammad Abrar. 2023. “Deep Learning Techniques for Web-Based Attack Detection in Industry 5.0: A Novel Approach.” *Technologies 2023, Vol. 11, Page 107* 11 (4): 107. https://doi.org/10.3390/TECHNOLOGIES11040107.

[15] Velasquez, David, Enrique Perez, Xabier Oregui, Arkaitz Artetxe, Jorge Manteca, Jordi Escayola Mansilla, Mauricio Toro, Mikel Maiza, and Basilio Sierra. 2022. “A Hybrid Machine-Learning Ensemble for Anomaly Detection in Real-Time Industry 4.0 Systems.” *IEEE Access* 10: 72024–36. https://doi.org/10.1109/ACCESS.2022.3188102.

[16] Wang, Xiaoding, Sahil Garg, Hui Lin, Jia Hu, Georges Kaddoum, Md Jalil Piran, and M. Shamim Hossain. 2022. “Toward Accurate Anomaly Detection in Industrial Internet of Things Using Hierarchical Federated Learning.” *IEEE Internet of Things Journal* 9 (10): 7110–19. https://doi.org/10.1109/JIOT.2021.3074382.

[17] Wu, Huanzhuo, Yunbin Shen, Xun Xiao, Giang T. Nguyen, Artur Hecker, and Frank H.P. Fitzek. 2023. “Accelerating Industrial IoT Acoustic Data Separation With In-Network Computing.” *IEEE Internet of Things Journal* 10 (5): 3901–16. https://doi.org/10.1109/JIOT.2022.3176974.

[18] Yang, Kaixiang, Yifan Shi, Zhiwen Yu, Qinmin Yang, Arun Kumar Sangaiah, and Huanqiang Zeng. 2023. “Stacked One-Class Broad Learning System for Intrusion Detection in Industry 4.0.” *IEEE Transactions on Industrial Informatics* 19 (1): 251–60. https://doi.org/10.1109/TII.2022.3157727.