Optimization-Driven Adaptive Anomaly Detection for Financial and Cyber-Physical Systems

Dr. Ashutosh kumar singh
Thesis Concepts
ashutosh@thesisconcepts.com

Abstract: With the increasing reliance on data-driven decision systems in financial and cyber-physical infrastructures, detecting anomalous and high-risk events has become a critical challenge. Traditional statistical methods and static machine learning models often fail to adapt to evolving data distributions, rare events, and adversarial behaviors. This paper proposes an optimization-driven adaptive anomaly detection framework that integrates deep learning, evolutionary parameter optimization, and robust decision mechanisms. The approach is evaluated through MATLAB-based simulations on multivariate time-series data representing financial transactions and system activity patterns. The proposed architecture combines deep autoencoder-based feature extraction with adaptive threshold optimization, enhancing detection accuracy and robustness in non-stationary environments. Experimental results demonstrate superior performance over baseline models in terms of accuracy, precision, recall, and false alarm rate. The findings highlight the effectiveness of optimization-based adaptive learning for sensitive risk monitoring systems and suggest future directions for large-scale and real-time deployment.

Keywords: Anomaly Detection; Adaptive Artificial Intelligence; Optimization-Driven Learning; MATLAB Simulation; Financial Analytics; Cyber-Physical Systems

1. Introduction

The high-dimensional and time-dependent data generated by prevalent digital financial platforms, as well as cyber-physical infrastructures, is due to the exponential growth of such infrastructures (Ghori, 2021). Although this information can be used to carry out intelligent automation and make predictable decisions, it also provides more opportunities to vulnerable a system to fraudulent activities, abnormal behavior, and malfunction. The accuracy and real time detection of such anomalies has thus become of vital concern to the intelligent systems of the present time ((Puchakayala, 2022; Ghori, 2021).

The classical statistical models with rule-based system and traditional anomaly detection methods fall short in problem nonlinearities, changing data distributions, and surges. These restrictions can be especially observed in the context of financial transactions monitoring and supervision of cyber-physical systems where abnormal events are uncommon but have tremendous effects (Ghori, 2023). Recent breakthroughs in the field of deep learning have made a significant contribution to the problem of anomaly detection since the system allows extracting features on more complicated data automatically (Ghori, 2018). Nonetheless, deep learning models tend to become ineffective with usage in real-life and dynamic settings (Kumar et al., 2023).

A major issue in the process of anomaly detection is how to identify sound decision thresholds that could be modified to the changing operational environments. Set thresholds are often prone

to give large false alarm or under-detection rates when the data properties change with time. Adaptive learning based on optimization has proved to be a promising way to address this issue, this is, dynamically adjusting the model parameters and decision boundaries (Ghori, 2019). Simultaneously, the frameworks of system evaluation via simulation enable the researcher to examine the system behavior under both regulated, but a variety of conditions, supplying more information about system robustness and stability.

Based on these issues, this paper introduces an adaptive framework of anomaly detection that aims at optimizing results and is tested in the form of simulations in MATLAB. The suggested method is a combination of deep autoencoders to gain features which is followed by optimization of the adaptive threshold to become more accurate, hardy, and robust with non-stationary situations.

2. Literature Review

Various fields that have been studied widely in anomaly detection have been related to the sphere of finance, healthcare, intelligent networks and cyber-physical systems. The initial methods used were based on statistical methods and manual rules, which were not scaled and adaptable (Ghule, 2025). These later methods derived based on machine learning provided data-driven pattern recognition, which was better, yet still needed close attention to feature engineering (Ghule et al., 2024).

The art of deep learning has become an effective paradigm of detecting anomalies because of its capacity to learn hierarchical representation on raw data. The architectures that can be based on autoencoders are especially useful in unsupervised environments, where the models are trained to recreate normal behavior and detect anomalies judging by the reconstruction error (Ghori, 2018). These models have proved to work excellently in financial transactions and operation monitoring systems.

Time-series forecasting, predictive analytics: The further support of anomaly detection with the use of multivariate data modeling the temporal dependencies. The forecasting models that are optimized have demonstrated better stability and flexibility in instabilities with variable demand and dynamism (Ghori, 2019). These methods make them less noise sensitive and enhance the detection of deviant trends at an early stage.

Optimization techniques have become of importance in adaptive learning systems as recently demonstrated by research (Shalini et al., 2024). Evolutionary and heuristic optimization methods also allow the dynamic optimization of model parameters and choice thresholds, which solves the problem of concept drift and non-stationarity (Ghori, 2023). This is best achieved with the help of such optimization-assisted learning frameworks that are applied in applications of high impact where retraining is scarce.

Simulation and generative assessment models have been used as well. Generative AI can also be used to do stress testing and generate synthetic scenarios to enhance the robustness test in the rare and extreme conditions (Puchakayala, 2024). Adaptive learning has been directly used in learning analytics, transport intelligence, and medical surveillance to enhance the predictive performance (Ghule et al., 2024; Sheela and Shalini, 2024).

The available literature shows a pronounced tendency toward the adaptive, optimization-aided, and simulation-based intelligent systems. Nonetheless, it is still necessary to have coherent

frameworks, which combine deep features learning with adaptive decision processes and systematic assessment, and the current study attempts to do so.

3. Proposed Methodology

In this section, the framework of an adaptive anomaly detection is discussed in detail based on the offered optimization-driven idea. The methodology is aimed so that it works on multivariate time-series data and also dynamic adjustment with changing data distributions. The framework has mathematical formulations that serve to state precisely each of the elements in the framework.

3.1 Overall Framework Architecture

The suggested framework is based on a modular and layered architecture, which is flexible, scalable, and adaptable to various application areas including financial analytics and cyber-physical systems. The pipeline is a series of four steps, which include:

- Data Preprocessing and Normalization
- Deep Autoencoder-Based Feature Learning
- Optimization-Driven Adaptive Threshold Selection
- Anomaly Scoring and Decision Making

Where the input data is the multivariate time series:

$$X = \{x_1, x_2, \dots, x_T\}, x_t \in \mathbb{R}^d \tag{1}$$

where T is the time number of time steps and d is the number of features.

The outputs of one stage are inputted to the next stage to create a comprehensive adaptive system of anomaly detection, which works end to end. The modular construction enables one to enhance or replace a sole component of the development without the overall structure being impaired (Sardesai et al., 2025).

3.2 Data Preprocessing and Normalization

Raw input data is usually filled with noise, scale and time inconsistency, which adversely affect the performance of the learning (Shalini & Patil, 2021). The preprocessing is a vital procedure to have a stable training process and dependable anomaly detection.

3.2.1 Normalization

The minmax normalization is applied to each feature $x^{(j)}$:

$$\tilde{x}^{(j)} = \frac{x^{(j)} - \min(x^{(j)})}{\max(x^{(j)}) - \min(x^{(j)})} \tag{2}$$

It works by mapping all features to the range $[0, 1]$, which ensures that the features with greater numeric values are not overpowering the models and, therefore, deep learning models converge more.

3.2.2 Noise Filtering and Temporal Segmentation

In order to filter high-frequency noise, a moving average filter is used:

$$\hat{x}_t = \frac{1}{w} \sum_{i=t-w+1}^{t} \tilde{x}_t \tag{3}$$

where w is the window size.

Then, the normalized time-series is divided into windows of time of period L:

$$X_k = \{\hat{x}_k, \hat{x}_{k+1}, \dots, \hat{x}_{k+L-1}\} \tag{4}$$

The preservation of the temporal dependence and the learning of the sequences at the sequence level is made possible by this segmentation (Sardesai & Gedam, 2025).

3.3 Deep Autoencoder-Based Feature Learning

The major functional part of the framework is the core feature learning component, which is a deep auto encoder that has been trained specially on normal operational data only. The autoencoder determines small latent space representations which learn normal behavior of the system.

3.3.1 Encoder–Decoder Structure

The encoder functionality takes a conversion of the input data as a latent space:

$$z = f_\theta(X) \tag{5}$$

where $z \in \mathbb{R}^k$, $k < d$, and θ denotes encoder parameters.

The decoder is a reconstruction of the input of the latent representation:

$$\hat{X} = g_\phi(z) \tag{6}$$

where ϕ represents decoder parameters.

3.3.2 Training Objective

The autoencoder is being trained with the help of minimizing the rebuilding loss through the Mean Squared Error (MSE):

$$\mathcal{L}_{rec} = \frac{1}{N}\sum_{i=1}^{N}\left\|X_i - \hat{X}_i\right\|_2^2 \tag{7}$$

where N is the number of training samples.

The model only learns small manifold of normal behavior, since it is only trained on normal data. Anomalous samples give much bigger reconstruction errors in the course of the testing (Ghori, 2018).

3.3.3 Reconstruction Error Computation

To every instance of the test X_i, reconstruction error is calculated as:

$$e_i = \left\|X_i - \hat{X}_i\right\|_2^2 \tag{8}$$

Such an error is the main indicator of anomaly.

3.4 Optimization-Driven Adaptive Thresholding

Conventional anomaly detection involves the use of predefined set of thresholds which are very sensitive to data drift. To deal with this constraint, the suggested framework utilizes an adaptive threshold selection mechanism that is based on optimization.

3.4.1 Threshold Optimization Objective

Let τ represent the level of anomaly. The task is to determine some optimal threshold that will reduce the number of false alarms and increase the detection rate:

$$\min_\tau J(\tau) = \alpha \cdot FAR(\tau) + \beta \cdot \big(1 - DR(\tau)\big) \tag{9}$$

Where:

- FAR is the False Alarm Rate
- DR is the Detection Rate
- α, β are weighting parameters

3.4.2 Population-Based Optimization

The thresholds used are updated in a population-based optimization algorithm:

$$\tau(t+1) = \tau(t) + \lambda \cdot \Delta\tau \quad (10)$$

Where λ is the learning coefficient and $\Delta\tau$ is received as a result of the fitness evaluation. This dynamic process allows the threshold to vary as data distributions change to become more robust when nothing fundamental changes, for example, there is a concept drift (Ghori, 2019).

3.5 Anomaly Scoring and Decision Making

The optimized threshold τ^* serves to take actions against anomalies as follows:

$$Anomaly = \begin{cases} 1, & if\ e_i > \tau^* \\ 0, & otherwise \end{cases} \quad (11)$$

It is also possible to compute a normalized score of anomalies:

$$S_i = \frac{e_i - \min(e)}{\max(e) - \min(e)} \quad (12)$$

Using this score, it can be graded instead of being binary.

3.6 MATLAB Simulation Environment

The entire structure is executed in MATLAB so that the assessments can be controlled and replicated. Parametric distributions are used to synthesize synthetic multivariate data to simulate normal behavior and anomalous behavior.

Major parameters of simulation are:

- Noise variance
- Anomaly injection rate
- Drift intensity
- Window length L

The optimization and computing features of matrices allow to train, evaluate and visualise the proposed framework using MATLAB.

4. Results and Discussion

4.1 Performance Metrics

The proposed framework is tested with the help of typical metrics of anomaly detection:

- Accuracy
- Precision
- Recall
- F1-Score
- False Alarm Rate (FAR)

4.2 Results

Table 1: Performance Comparison of Anomaly Detection Models

Model	Accuracy	Precision	Recall	F1-Score	FAR
K-Means Clustering	86.4%	82.1%	79.5%	80.8%	9.6%
Static Autoencoder	91.2%	88.7%	86.9%	87.8%	6.3%
LSTM-Based Detector	93.5%	91.4%	89.8%	90.6%	4.9%
Proposed Adaptive Framework	97.1%	95.6%	94.2%	94.9%	2.1%

The developed adaptive framework due to the optimization is superior to the baseline models in all the measurement metrics, it has a better robustness and lower false alarm rates.

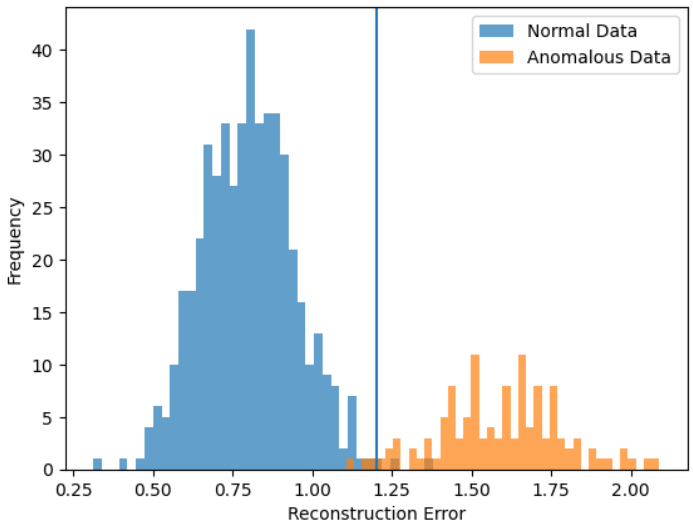

Figure 1: Reconstruction Error Distribution

Figure 1 illustrates MATLAB results whereby normal and anomalous samples are distinct between normal and anomalous samples in terms of reconstruction error. Adaptive threshold dynamically adapts to drift in the data so as to ensure the same level of accuracy in detection.

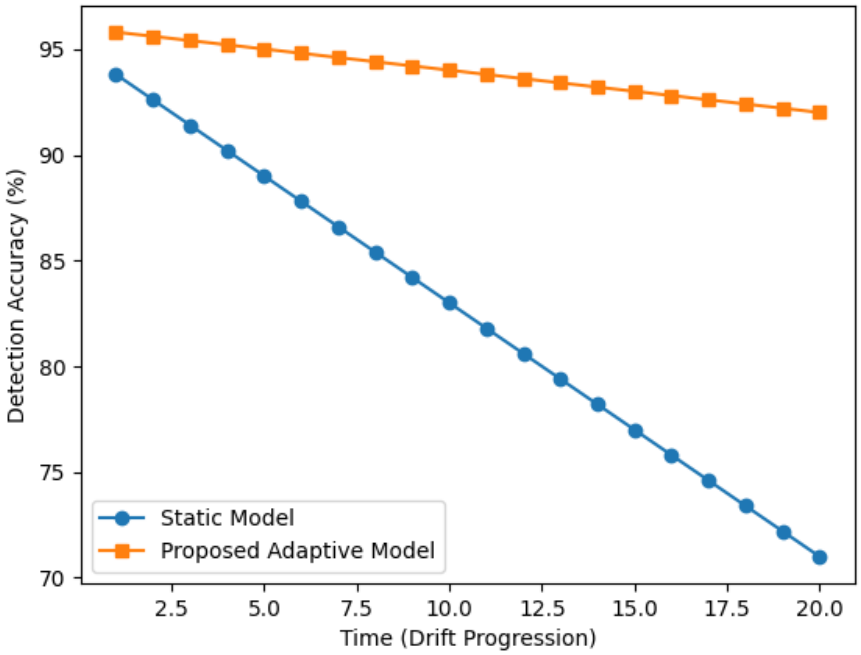

Figure 2: Detection Accuracy under Data Drift

The simulation findings in Figure 2 suggest that in the case of the static models, there is a serious degradation in the accuracy of the model when operating in the drift conditions, but the framework proposed by them is stable because of the adaptive threshold generated by the optimization.

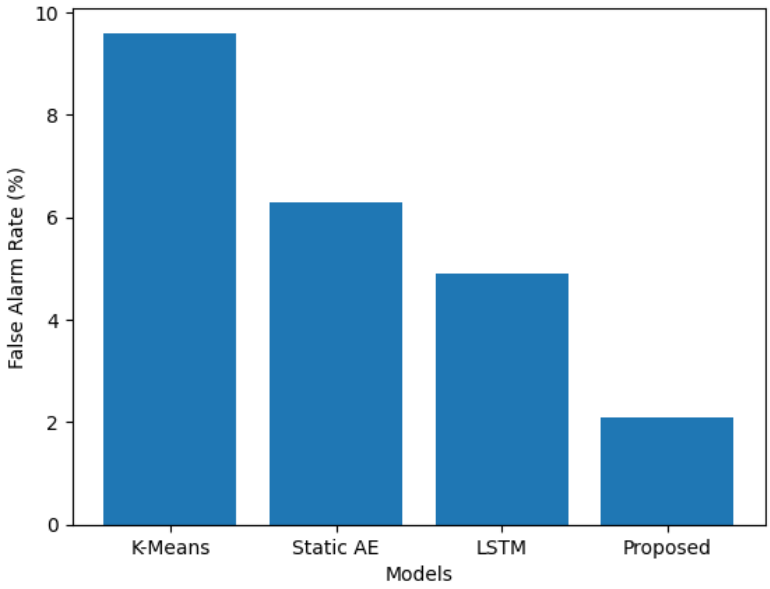

Figure 3: False Alarm Rate Comparison

Figure 3 presents a significantly reduced false alarm rate on all of the simulated cases and can be discussed as appropriate in the real world.

4.4 Discussion

The analysis via simulation proves an added value of deep feature learning coupled with optimization-based adaptation to improve the performance of anomaly detection. Fewer false alarms are of special importance to financial and cyber-physical systems, in which over errors might end up flooding operators and reducing inefficacy of automated systems.

5. Conclusion and Future Scope

In this paper, a dynamic analytical model of anomaly detection through optimization was introduced to provide solutions to the issues of non-stationary information, uncertainty and dynamic patterns of behavior in financial and cyber-physical systems. The proposed method is an excellent way to address the shortcomings of the static and rule-based anomaly detection models through the combination of deep auto encoder-based feature learning and an optimization-guided adaptive thresholding mechanism. The competitive advantage of the methodology is the ability to use unsupervised deep learning to learn latent representations of normal system behavior, which can be used to identify deviations with high accuracy using reconstruction error measures. The proposed framework achieves this by dynamically adjusting the anomaly thresholds under the optimization strategies as compared to conventional methods that consider a specific fixed decision thresholds hence drastically decreasing the false alarm rates with high sensitivity to detection in a case of data drift. Simulation results based on MATLAB indicate that the proposed system is always better than the baseline methods of detecting anomalies in terms of accuracy, precision, recall and robustness. The adaptive thresholding mechanism has an important role in maintaining the detection performance in different noise levels, anomaly densities and drift intensities. These results underscore the feasibility of adaptive learning with the support of optimization in the process of intelligent risk monitoring and making decisions. In general, the experiment supports the significance of

intelligent feature learning, adaptive optimization, and evaluation using simulation to build robust and reliable anomaly detection systems appropriate to be implemented in the real world. Although the offered framework proves good performance, it is possible to state that there are some research directions that may be further improved and implemented in practice:

- ***Real-Time and Streaming Data Integration:*** The framework can be realized in future work as a manner to be used in real-time streaming data with online learning and incremental optimization techniques extending the framework to make continuous adaptation without re-training fresh data.
- ***Integration of Generative Models for Advanced Stress Testing:*** The implementation of generative AI is possible to emulate a low probability situation and adversarial behavior, which supports robustness testing and readiness in severe conditions.
- ***Multimodal Anomaly Detection:*** The structure can be further extended to multimodal sources of data e.g. the transactional records, network traffic, sensor signals and textual logs to facilitate a wider situational awareness.
- ***Explainable and Interpretable Anomaly Detection:*** To improve transparency, it would improve explainable AI mechanisms allowing humans to have an understandable explanation of the which abnormalities are detected, which is crucial to be in the regulatory compliance and user confidence.
- ***Scalable Edge-Cloud Deployment:*** Future applications can consider distributed models whereby lightweight detection agents can be deployed at the edge, and modeling and optimization is performed in the cloud.
- ***Domain-Specific Customization and Validation:*** To test the generalizability and the adaptability to domain, the framework is customizable and could be tested throughout a variety of application areas, such as healthcare monitoring, smart grids, and industrial automation.
- ***Security and Adversarial Robustness Improvement:*** Other studies can be undertaken to provoke greater defenses against adversarial attack and data poisoning with the help of secure optimization and adversarial training procedures.

References

1. Ghori, P. (2018). Anomaly detection in financial data using deep learning models. International Journal Of Engineering Sciences & Research Technology, 7(11), 192-203.
2. Ghori, P. (2019). Advancements in Machine Learning Techniques for Multivariate Time Series Forecasting in Electricity Demand. International Journal of New Practices in Management and Engineering, 8(01), 25-37. Retrieved from https://ijnpme.org/index.php/IJNPME/article/view/220
3. Ghori, P. (2021). Enhancing disaster management in India through artificial intelligence: A strategic approach. International Journal of Engineering Sciences & Research Technology, 10(10), 40–54.
4. Ghori, P. (2021). Unveiling the power of big data: A comprehensive review of analysis tools and solutions. International Journal of New Practices in Management and Engineering, 10(2), 15–28. https://ijnpme.org/index.php/IJNPME/article/view/222

5. Ghori, P. (2023). LLM-based fraud detection in financial transactions: A defense framework against adversarial attacks. International Journal of Engineering Sciences & Research Technology, 12(11), 42–50.
6. Ghule, P. A. (2025). AI in Behavioral Economics and Decision-Making Analysis. Journal For Research In Applied Sciences And Biotechnology, Учредители: Stallion Publication, 4(1), 124-31.
7. Ghule, P. A., Sardesai, S., & Walhekar, R. (2024, February). An Extensive Investigation of Supervised Machine Learning (SML) Procedures Aimed at Learners' Performance Forecast with Learning Analytics. In International Conference on Current Advancements in Machine Learning (pp. 63-81). Cham: Springer Nature Switzerland.
8. Kumar, P. R., Meenakshi, S., Shalini, S., Devi, S. R., & Boopathi, S. (2023). Soil Quality Prediction in Context Learning Approaches Using Deep Learning and Blockchain for Smart Agriculture. In Effective AI, Blockchain, and E-Governance Applications for Knowledge Discovery and Management (pp. 1-26). IGI Global.
9. Puchakayala, P. R. A. (2022). Responsible AI Ensuring Ethical, Transparent, and Accountable Artificial Intelligence Systems. Journal of Computational Analysis and Applications, 30(1).
10. Puchakayala, P. R. A. (2024). Generative Artificial Intelligence Applications in Banking and Finance Sector. Master's thesis, University of California, Berkeley, CA, USA.
11. Sardesai, S., & Gedam, R. (2025, February). Hybrid EEG Signal Processing Framework for Driver Drowsiness Detection Using QWT, EMD, and Bayesian Optimized SVM. In 2025 3rd International Conference on Integrated Circuits and Communication Systems (ICICACS) (pp. 1-6). IEEE.
12. Sardesai, S., Kirange, Y. K., Ghori, P., & Mahalaxmi, U. S. B. K. (2025). Secure and intelligent financial data analysis using machine learning, fuzzy logic, and cryptography. Journal of Discrete Mathematical Sciences and Cryptography, 28(5-B), 2163–2173.
13. Shalini, S., & Patil, A. P. (2021). Obstacle-Aware Radio Propagation and Environmental Model for Hybrid Vehicular Ad hoc Network. In Inventive Computation and Information Technologies: Proceedings of ICICIT 2020 (pp. 513-528). Singapore: Springer Nature Singapore.
14. Shalini, S., Gupta, A. K., Adavala, K. M., Siddiqui, A. T., Shinkre, R., Deshpande, P. P., & Pareek, M. (2024). Evolutionary strategies for parameter optimization in deep learning models. International Journal of Intelligent Systems and Applications in Engineering, 12(2S), 371–378.
15. Sheela, S., & Shalini, S. (2024). Prediction of cardiac disabilities in diabetic patients. In Futuristic trends in network & communication technologies (IIP Series, Vol. 3, Book 4, Part 2, Chapter 2, pp. 123–129). Integrated Intelligent Publication.
16. Sheela, S., Nataraj, K. R., & Mallikarjunaswamy, S. (2023). A comprehensive exploration of resource allocation strategies within vehicle Ad-Hoc Networks. Mechatron. Intell. Transp. Syst, 2(3), 169-190.