Anomaly Detection Frameworks Taxonomy

Imelda Zadeja, Kaspars Osis

Vidzeme University of Applied Sciences, Valmiera, Latvia

Introduction

In recent years, the increase of digital systems and the consequent need for data volumes have amplified the demand for intelligent systems capable of autonomous monitoring and decision-making. Anomaly detection, the process of identifying patterns in data that deviate significantly from expected behaviour (Chandola, 2009), plays a crucial role in applications such as fault detection, cybersecurity, predictive maintenance, and fraud detection (Nassif A, 2021). However, the increasingly complex nature of modern systems presents challenges in designing anomaly detection frameworks that are scalable and adaptable across various contexts (M. R. Alam, 2019). This research introduces a taxonomy of anomaly detection frameworks, focusing on their capabilities, design dimensions, and levels of abstraction. The proposed taxonomy aims to guide the evaluation of existing frameworks and the design of solutions that are robust, interpretable, and deployable in real-world environments.

Methods

This research adopts a comprehensive and systematic literature review of state-of-the-art anomaly detection frameworks over the last ten years. Literature was retrieved from major databases, including Scopus and Web of Science. Frameworks are included if they had a Field-Weighted Citation Impact (FWCI) greater than five, to ensure that highly influential and peer-recognized works were considered in this research, and the frameworks selected have added significant value in the field. Eight frameworks are ultimately selected, representing a diverse set of application domains such as cybersecurity, cloud infrastructure, logistics, and IoT systems. The aim is to identify, organize, and evaluate the core capabilities and design principles that support these frameworks. Based on the literature, the research extracts architectural and functional components, which are then synthesized into an anomaly detection framework taxonomy. Moreover, the study introduces the concept of framework abstraction levels, distinguishing between frameworks that are highly domain-specific, cross-domain adaptable, or designed with domain-agnostic generalization. This abstraction perspective allows for the evaluation of how flexibly a framework can be transferred across contexts, and how granular its architecture is in supporting different types of anomaly detection scenarios.

Results

The research results in the formulation of a structured taxonomy for anomaly detection frameworks. Eight influential frameworks were analysed to extract key characteristics and design patterns. The taxonomy comprises multiple dimensions, including: [1] Anomaly detection techniques, [2] Data type compatibility, [3] Scalability and performance optimization, [4] Explainability and interpretability, and [5] Domain specificity. These dimensions were synthesized into a hierarchical schema that comprises the core features. This taxonomy allows for horizontal comparison across domains and vertical comparison within framework complexity.

Conclusions and Future Work

This study presents a novel taxonomy and abstraction model that provides a systematic, comparative perspective on the diversity and complexity of contemporary anomaly detection frameworks. The taxonomy facilitates critical assessment of existing solutions and supports the development of more effective, domain-adaptable systems through the synthesis of key capabilities and architectural patterns.

Future research directions recommend the involvement of the following aspects:

Developing technical requirements specifications for the anomaly detection frameworks.

Evaluating data quality requirements and their impact on anomaly detection efficacy.

Assessing security requirements for the deployment of anomaly detection frameworks.

Comparative analysis with existing classification approaches will have to be also undertaken to refine the taxonomy's structure and to further enhance its relevance for academic and industry applications.

References

Chandola, V. B. (2009). Anomaly Detection: A survey. *ACM Computing Surveys, 41*(3), 1-58. https://doi.org/10.1145/1541880.1541882

M. R. Alam, I. G. (2019). A Framework for Tunable Anomaly Detection. *IEEE International Conference on Software Architecture (ICSA)*, 201-210. https://doi.org/10.1109/ICSA.2019.00029

Nassif A, T. M. (2021). Machine Learning for Anomaly Detection: A Systematic Review. *IEEE Access, 9*, 78658-78700. https://doi.org/10.1109/ACCESS.2021.3083060

Keywords

anomaly detection, anomaly detection framework, anomaly detection taxonomy