Enhancing Anomaly Detection: Innovative Approaches for Accurate and Efficient Detection

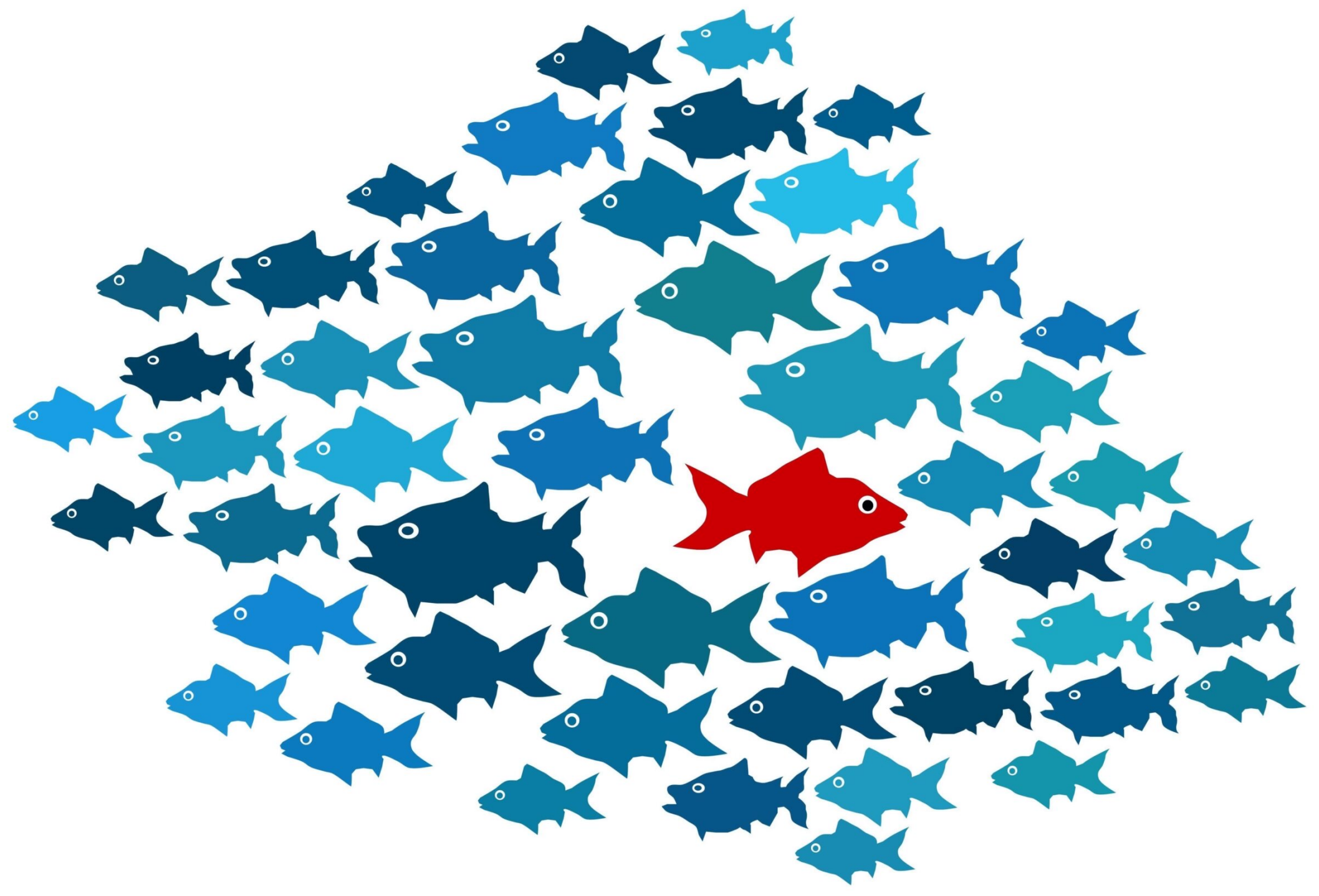
Samir Kanbar and Daniel Schwartz
Department of Computer Science, Florida State University, Tallahassee, FL, 32303

Abstract

Anomaly detection is essential for identifying irregular patterns that may indicate security threats, system malfunctions, or medical anomalies. Industries such as cybersecurity, healthcare, and finance rely on accurate detection methods to prevent fraud, diagnose diseases, and enhance system reliability. This research explores innovative techniques for improving anomaly detection accuracy and efficiency, leveraging machine learning, rule-based systems, and hybrid approaches. By designing a structured framework for data collection, preprocessing, and model evaluation, this study aims to enhance detection capabilities. Through visual analyses and performance comparisons, the research highlights key insights and future directions, contributing to the advancement of robust anomaly detection systems.

Conclusion

While initial experimentation lays the groundwork for the research by collecting data and sources to develop a clear understanding of what anomaly-detection based systems are, there is more of a focus on future work that involves testing these systems in real-world scenarios. A mix of testing different plans and “missions” while defining what certain anomalies in the process are in this stage of the research is crucial to developing these systems in the future. Key challenges, such as data limitations and model optimization, will be addressed by integrating more advanced algorithms and refining feature selection techniques. By continuously iterating on these methods, this study aims to contribute to more robust and reliable anomaly detection systems, paving the way for practical implementation in critical domains.



Resources

Chandola, Vipin, Arvind Kumar, and V. S. Lakshmanan. "Anomaly Detection: A Survey." *ACM Computing Surveys*, vol. 41, no. 3, 2009, pp. 1-58.

Ahmed, Mohammed, et al. "A Survey of Network Anomaly Detection Techniques." *International Journal of Computer Applications*, vol. 17, no. 1, 2011, pp. 1-19.

Xia, Yuliang, et al. "Hybrid Deep Learning Models for Anomaly Detection." *Journal of Machine Learning Research*, vol. 19, no. 1, 2018, pp. 1-28.

Methodology

To execute this study, a combination of machine-learning and rule-based approaches are employed to create an effective anomaly detection system. The methodology of this research begins with collecting data from relevant peer reviewed sources on what defines anomalies, what devices are used already to answer this research question, and what are the most effective ways to detect anomalies and replan. Through this research, various algorithms are trained to execute these tasks through precision and accuracy metrics. As well, a rule-based system is implemented to detect predefined anomalies while hybrid approaches are used to improve detection performance. This experimental setup uses Python and frameworks like TensorFlow with structured pipelines for model training, validation, and testing.

Future Directions

To advance anomaly detection, future research can explore several promising areas. First, integrating deep learning models, such as autoencoders and recurrent neural networks (RNNs), could improve detection accuracy for complex and high-dimensional data. Additionally, optimizing algorithms for real-time anomaly detection is crucial for applications in cybersecurity and healthcare, where immediate responses are essential. Another avenue for improvement lies in hybrid models that combine machine learning with reinforcement learning, enabling adaptive systems that continuously learn and refine detection capabilities. Further research in these areas could enhance the robustness and efficiency of anomaly detection across diverse industries.