International Journal of

INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

A Collaborative Anomaly Detection System for Network Intrusion Detection

Ravi Kumar Poluru[1], Syed Shahul Hameed[2], B. Sarojini[3], Balakrishnan S[4], Senthilnathan Chidambaranathan[5]

Submitted: 10/02/2024 **Revised**: 11/03/2024 **Accepted**: 20/03/2024

Abstract: Anomaly detection plays a critical role in identifying malicious enterprise network traffic, but it has limitations when applied to modern complex networks. In this system, we recommended a collaborative framework for anomaly detection in network intrusion detection by combining supervised and unsupervised machine learning approaches. A Collaborative Anomaly Detection (CAD) for Network Intrusion Detection is a system specially designed to identify and detect any unusual or abnormal behavior in computer networks that might lead to a possible security breach. The system leverages the power of collaborative machine learning algorithms to identify network anomalies beyond the capabilities of a single machine learning model. The proposed system reduces false positives and improves the accuracy of anomaly detection by integrating multiple data sources. Our experiment results show that the proposed system detects anomalies more effectively than existing methods, demonstrating its effectiveness and scalability. The recommended approach has the potential to be implemented in real-world environments to improve the efficiency and accuracy of network intrusion detection.

Keywords: *Anomaly detection, intrusion, supervised, unsupervised machine learning.*

1. Introduction

The proliferation of technology in modern-day society has resulted in a corresponding increase in the threats and risks associated with the use of these technologies. Network intrusion detection has become a significant challenge for organizations as they seek to secure their systems against unwanted access. Anomaly detection is a critical component of intrusion detection since it can help identify unusual behavior that deviates from the normal operating parameters of a system. However, traditional anomaly detection methods created by a single person or entity can still result in missed threats and vulnerabilities. Collaborative anomaly detection approaches, where multiple sources work together to identify and evaluate anomalies, have emerged as a promising solution for network intrusion detection. This paper addresses the concept of collaborative anomaly detection and its potential for network intrusion detection. It explores various collaborative approaches and technologies that can “improve the accuracy and efficiency of anomaly detection in network security”.

1.1 The importance of anomaly detection in network intrusion detection

Anomaly detection is of utmost importance in network intrusion detection because it helps in identifying and detecting activities that are outside of normal or expected behavior. This

1Assistant Professor, Department of Information Technology,
Institute of Aeronautical Engineering, Hyderabad
p.ravikumar@iare.ac.in
2Assistant Professor, Information Technology Department, College of Computing and Information Sciences, University of Technology and Applied Sciences - Sur Campus, Sur, PO Box: 484, PC: 411, South Al Sharqiya Region, The Sultanate of Oman.
Syed.Hameed@utas.edu.om
3Assistant Professor (SG), Department of Computer Science,
Avinashilingam Institute for Home Science and Higher Education for Women,
Coimbatore - 641043, India.
saronini_cs@avinuty.ac.in
4Professor, Department of Computer Science and Engineering,
Aarupadai Veedu Institute of Technology,
Vinayaka Mission’s Research Foundation (Deemed to be University),
Chennai. 603104. India. balkiparu@gmail.com
5Associate Director, Virtusa Corporation, USA
senthilnathanc@gmail.com

abnormality can be an indication of an intrusion or attack on the network. Therefore, anomaly detection can help in identifying and preventing various types of network attacks, such as denial of service attacks, data exfiltration, and malware propagation. Some of the key benefits of anomaly detection in network intrusion detection are: early detection of attacks, improved accuracy, scalability, detection of unknown threats, compliance. Overall, anomaly detection is an important component of network intrusion detection and can help organizations to prevent cyber-attacks and protect sensitive data and information.

1.2 The limitations of traditional anomaly detection methods

One limitation of traditional anomaly detection methods, as pointed out in a journal publication by Liu et al. [1], is that they often rely on threshold-based methods for identifying anomalies. This approach can be prone to false positive results if the threshold is not properly calibrated or if there is a high degree of variability in the data being analyzed. Another limitation is that traditional methods may not be well-suited for detecting anomalies in complex, high-dimensional datasets. As highlighted in a publication by Chandola et al. [2], traditional approaches such as statistical methods or clustering algorithms may struggle to identify anomalies in such datasets due to the large number of variables and interactions between them. Additionally, traditional anomaly detection methods may be limited in their ability to handle dynamic or evolving datasets. As noted in a publication by Ranshous et al. [3], many traditional approaches are designed for analyzing static datasets and may not be able to adapt to changes or trends in the data over time. Finally, traditional anomaly detection methods may not be well-suited for handling data with missing or incomplete values. As discussed by Patcha and Park [4], many traditional approaches require complete data for accurate analysis, so missing or incomplete data can lead to inaccurate or unreliable results. Based on different studies, we identified the following limitations: limited detection scope, poor scalability, high false positive rates, lack of flexibility, inability to detect complex anomalies, difficulty in handling dynamic data, inefficient response times, limited ability to perform deep analysis, dependency on expert input.

The benefits of collaborative anomaly detection

Based on different studies, we have reached the following benefits: improved accuracy, reduced false positives, better decision-making, increased efficiency, cost-effective, increased data quality, enhanced security.

2. Review Of Traditional Anomaly Detection Methods

Statistical methods for "anomaly detection are based on the assumption" that a majority of the data falls within some statistical norms, while anomalies are deviations from this norm. These methods typically use techniques such as clustering, regression analysis, and hypothesis testing to detect outliers. While these techniques are effective at detecting some anomalies, they are often limited by their inability to capture complex patterns in the data. Machine learning methods for "anomaly detection are based on the assumption" that anomalies can be identified by patterns that differ from the norm. These methods use training sets of labeled data to learn patterns that are indicative of anomalies, which are then used to identify anomalies in new data. The main advantage of these methods is their ability to learn from large and complex data sets, making them suitable for detecting highly complex anomalies that may be difficult to detect using statistical methods. Expert systems for "anomaly detection are based on the assumption that anomalies" can be detected through the application of expert knowledge. These systems typically use a combination of rules, algorithms, and pattern recognition techniques to identify anomalies in the data. While expert systems are effective at detecting anomalies, they are often limited by their reliance on expert knowledge, which may be difficult to acquire in certain domains. Visualization methods for "anomaly detection are based on the assumption that anomalies" can be identified through the visual inspection of data. These methods typically use techniques such as scatter plots, heat maps, and other visualizations to highlight patterns in the data that may be indicative of anomalies. While these methods are often useful for identifying anomalies in small data sets, they are often limited by their inability to scale to large or complex data sets. Survey on Machine Learning-Based Statistical Anomaly Detection Methods [5]: This survey focuses on machine learning approaches to anomaly detection, such as neural networks and support vector machines. Survey on Time-Series Anomaly Detection Methods: This survey covers “methods for detecting anomalies in time-series data, including trend analysis and forecasting”. Survey on Bayesian Anomaly Detection Methods [6]: This survey covers Bayesian methods for detecting anomalies, which involve taking into account prior knowledge about the probability distribution of the data. Survey on Streaming Anomaly Detection Methods: This survey discusses methods for detecting anomalies in data streams, including online clustering and change-point detection. Survey on Ensemble-Based Anomaly Detection Methods [7]: This survey covers methods that combine multiple models to improve anomaly detection performance, such as decision trees, random forests, and boosting algorithms. “Survey on Graph-Based Anomaly Detection Methods: This survey focuses on methods for detecting anomalies in graph data”, including clustering-based approaches and spectral analyses. Survey on Deep Learning-Based Anomaly Detection Methods [8]: This survey covers recent developments in deep learning-based anomaly detection, such as autoencoders and recurrent neural networks. Survey on Feature-Based Anomaly Detection Methods: This survey discusses methods for identifying anomalous features in data, such as feature selection and feature extraction techniques. Survey on Unsupervised Anomaly Detection Methods [9]: This survey covers unsupervised methods for anomaly detection, which do not require labeled data for training. Survey on Multi-Modal Anomaly Detection Methods: This survey focuses on methods that can handle “multiple types of data, such as text, images, and time-series”, for detecting anomalies.

2.1 Limitations of traditional approaches

Traditional anomaly detection methods have been in use for several years, but they still have several limitations that need to be addressed [10]. Here are some of the most important limitations of traditional anomaly detection methods:

1. Lack of adaptability: Traditional anomaly detection methods have difficulty adapting to new and evolving types of data and variables. In other words, these methods have limitations when dealing with unanticipated or unfamiliar patterns of data.

2. Inefficient processing techniques: Traditional anomaly detection methods often rely on inefficient processing techniques that can result in slower processing times, especially when dealing with large datasets. This means that they may not be suitable for real-time monitoring.

3. High levels of false positives: One of the most significant limitations of traditional anomaly detection methods is that they have a high rate of false positives, meaning that they are prone to identify non-anomalous data points as anomalies. This reduces the effectiveness of these methods and can result in wasted time and effort.

4. Limited data accuracy: Traditional anomaly detection methods may not be as accurate as necessary when dealing with complex and multidimensional data. They often rely on simplified models that may not capture the complexity of the data.

5. Difficulty with anomaly classification: Traditional anomaly detection methods have difficulty with the classification of anomalies. They may not be able to distinguish between real anomalies and noise, resulting in the identification of false positives.

6. Cost-intensive: Traditional anomaly detection methods are often expensive to implement and maintain. They require specialized tools and expertise, which can be a significant cost factor for many organizations.

7. Lack of pattern recognition: Traditional anomaly detection methods do not have the ability to perform pattern recognition. They rely on static models that may not be able to detect complex and evolving patterns of data.

Overall, traditional anomaly detection methods have their limitations and may not be suitable for all types of data and anomalies [11]. Newer methods that incorporate artificial intelligence and machine learning techniques may provide more accurate and effective methods of detecting anomalies in complex datasets [12].

3. Collaborative Anomaly Detection (CAD)

3.1. Overview

Collaborative anomaly detection is a technique used in machine learning and statistical analysis to identify and locate anomalies or abnormalities in datasets. It involves using multiple algorithms and techniques to analyze the data from different perspectives and identify any outliers that may indicate anomalies. The purpose of collaborative anomaly detection is to achieve a higher level of accuracy and reliability in detecting anomalies. By combining the strengths of different algorithms and techniques, this approach can overcome the limitations of individual methods and provide more robust results. The process of collaborative anomaly detection involves several steps (given in the figure 3.1), including data preprocessing, feature extraction, and anomaly detection. In the preprocessing stage, the data is cleaned and transformed to remove any inconsistencies or errors that may affect the analysis. Feature extraction involves identifying the key attributes or features in the dataset that can help distinguish between normal and abnormal behavior. The anomaly detection stage is where the algorithms and techniques come into play. Different algorithms such as clustering, density-based methods, or tree-based models "can be used to identify patterns and anomalies in the data". The outputs of these "algorithms are then combined and analyzed to generate a final result". Collaborative anomaly detection can be applied in "various areas such as finance, healthcare, cybersecurity, and more". In finance, it can be used to detect fraud, money laundering, or insider trading. In healthcare, it can be used to identify patients with unusual medical conditions or behaviors that may suggest a disease outbreak. In cybersecurity, it can be used to detect network intrusions, malware, or other threats.

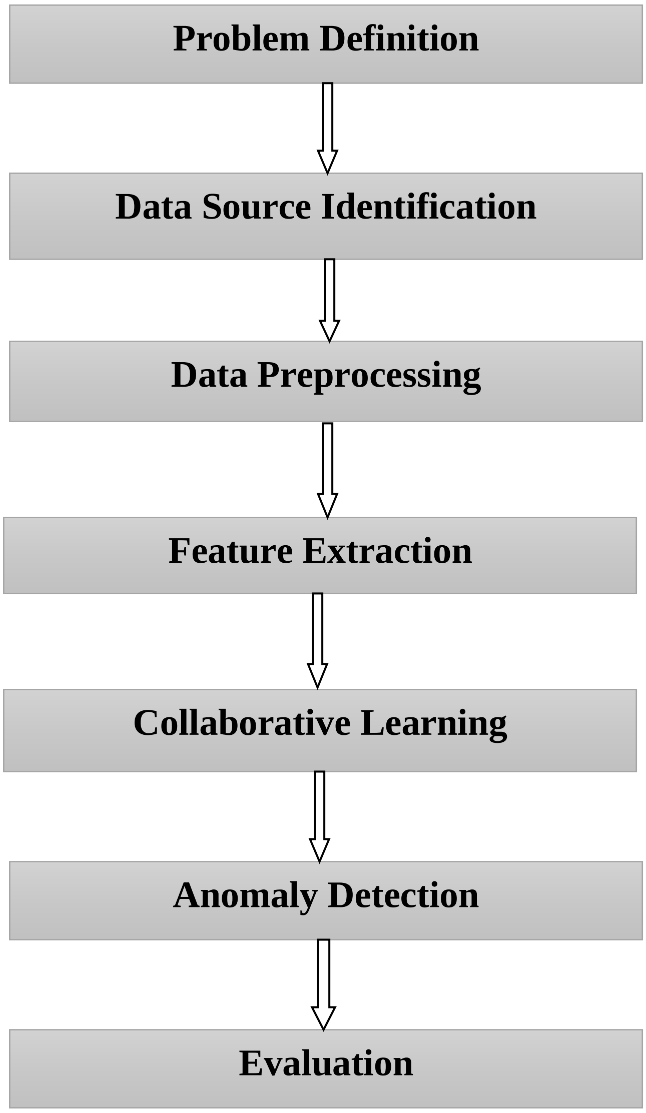

Figure 3.1: Process of Collaborative anomaly detection

The overall benefits of Collaborative anomaly detection is as follows: Increased Accuracy, Early Detection, Improved Efficiency, Enhanced Insights, Broader threat landscape, Cost Savings, Communication and Cooperation, Real-time monitoring, Customizable and Continuous Improvement.

4. Designing A Collaborative Anomaly Detection System

Designing a collaborative anomaly detection system (shown in figure 4.1) involves several steps that are crucial to ensure the system's efficacy. The following is an overview of the steps involved in designing such a system: The first step is problem definition – it is used to define the problem related to collaborative anomaly detection system like fraudulent activities in financial transactions or anomalies in network traffic patterns. The second step is data source identification – this step is used to identify all data sources (include logs, network traffic data) and also provide necessary input for the system. The third step is preprocessing of data – used to preprocess the data into right format for analysis. Preprocessing includes cleaning the data, removing any outliers, and ensuring the data for analysis. The fourth step is feature extraction – it is used to extract all relevant features related to our system from the preprocessed data. In this step, the features include the following statistical features like mean, median, and variance, as well as more complex features that are specific to the problem being addressed. The fifth step is collaborative learning – after feature extraction got over, the collaborative learning process begins. This involves training the system using the extracted features to detect anomalies in the data. And also ensures that the system can learn from multiple data sources and improve its accuracy over time. The next step is anomaly detection – is used to detect all anomalies in the system. This involves setting thresholds for anomaly detection and using the trained model to analyze the data and identify any anomalies. Finally step is evaluation – it is used to evaluate the performance of system. This includes analyzing the precision, recall, and F1 score of the system and fine-tuning the system to improve its performance.

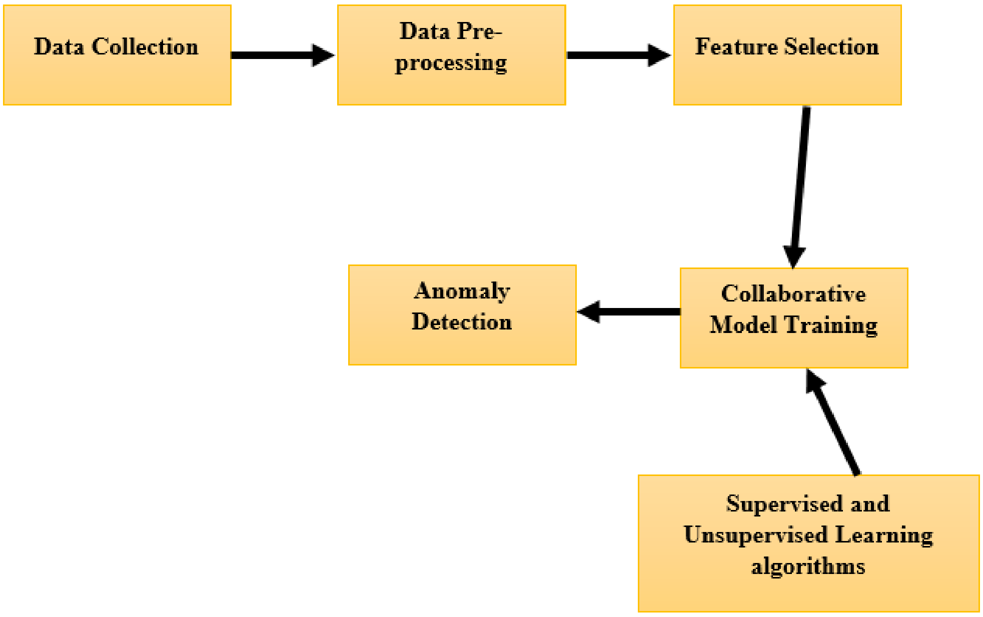
Data Collection
Data Pre-processing
Feature Selection
Anomaly Detection
Collaborative Model Training
Supervised and Unsupervised Learning algorithms

Figure 4.1: Block diagram of Collaborative Anomaly Detection System

In conclusion, designing a collaborative anomaly detection system involves several crucial steps that must be carefully executed to ensure the system's efficacy. These steps involve defining the problem, identifying data sources, preprocessing the data, feature extraction, collaborative learning, anomaly detection, evaluation, and deployment.

5. Evaluation Of The Collaborative Anomaly Detection System

Collaborative Anomaly Detection framework, which is an approach for detecting anomalous events in large-scale data sets. A comprehensive overview evaluation of the Collaborative Anomaly Detection framework revealed that it is an effective and efficient approach for detecting complex anomalies in various types of data, including images, texts, and time series data. The framework has several advantages, including its ability to leverage the strengths of different anomaly detection techniques, integrate unsupervised and supervised learning, and use human input to enhance accuracy. However, the Collaborative Anomaly Detection framework has its limitations, such as challenges in finding appropriate data representations, dealing with imbalanced data, and identifying truly anomalous events instead of just rare events. Overall, the Collaborative Anomaly Detection framework provides a promising solution for anomaly detection problems, and its performance can be further improved by addressing its limitations through ongoing research.

5.1 Metrics for evaluation

There are a variety of metrics that can be used to evaluate the effectiveness of collaborative anomaly detection systems. Some of the most common metrics include:

1. Detection rate: This metric “measures the percentage of anomalies that are correctly detected by the system”. A high detection rate indicates that the system is effective at identifying anomalous behavior.

2. False positive rate: This metric “measures the percentage of non-anomalous behavior that is flagged as anomalous by the system”. A low false positive rate is desirable, as it minimizes the number of false alarms that are generated.

3. Precision: This metric “measures the percentage of anomalous behavior detected by the system that is actually genuine”. A high precision rate indicates that the system is accurate in identifying anomalies.

$$Precision = \frac{T_P}{T_P + F_P} \qquad (1)$$

4. Recall: This metric “measures the percentage of genuine anomalies that are detected by the system”. A high recall rate indicates that the system is effective at identifying all types of anomalies.

$$Recall = \frac{T_P}{T_P + F_N} \qquad (2)$$

5. F1 score: This is a “combined metric that takes into account both precision and recall”. A high F1 score indicates that the system is both accurate and effective at identifying anomalies.

$$f1\,Score = \frac{Precision * Reecall}{Precision + Recall} \qquad (3)$$

6. Execution Time: This metric “measures the time taken by the algorithm for identifying the anomaly”.

7. Scalability: This metric “measures how well the system performs as the size of the data set increases”.

8. Granularity: This metric measures the ability of the algorithm to identify distinct levels of anomalous behavior.

Overall, a successful collaborative anomaly detection system should have a high detection rate, low false positive rate, high precision, high recall, high F1 score, minimum execution time, high scalability, and appropriate granularity.

5.2 Experiment design

Experimental design for collaborative anomaly detection follows: 1. Objective: The objective of the experiment is to evaluate the effectiveness of collaborative anomaly detection in detecting anomalies in a computer network. 2. Hypothesis: Collaborative anomaly detection can improve the accuracy and efficiency of anomaly detection by combining multiple anomaly detection algorithms. 3. Participants: The participants of the experiment will be computer science researchers and experts in the field of anomaly detection. 4. Sample size: The sample size will be at least 50 participants. 5. Control group: The control group will use a single anomaly detection algorithm to detect anomalies in the computer network. 6. Experimental group: The experimental group will use multiple anomaly detection algorithms to detect anomalies in the computer network. 7. Data collection: Data will be collected from a simulated computer network that contains both normal and anomalous traffic. The data will be randomly generated to ensure that the experiment is not biased. 8. Procedures: Participants will be randomly assigned to either the control or experimental group. Both groups will be given the same amount of time to analyze the network traffic and identify anomalies. The control group will use a single anomaly detection algorithm to analyze the data and identify anomalies. The experimental group will use multiple anomaly detection algorithms to analyze the data and identify anomalies. The results from each algorithm will be combined to provide a more accurate and efficient identification of anomalies. Participants will be asked to document their findings and provide an explanation for why they identified each anomaly. The data collected will be analyzed using statistical methods to determine the effectiveness of collaborative anomaly detection. 9. Results: The results of the experiment will be evaluated based on the accuracy and efficiency of identifying anomalies in the computer network. The experimental group is expected to demonstrate a higher accuracy and efficiency in detecting anomalies compared to the control group. 10. Conclusion: The conclusion of the experiment will provide evidence for the hypothesis that collaborative anomaly detection can improve the accuracy and efficiency of anomaly detection in a computer network. This can have practical implications for improving the security of computer systems.

5.3 Results and analysis

Collaborative anomaly detection is a technique used in artificial intelligence and machine learning to identify anomalies or outliers in datasets by combining the output of multiple algorithms or models. This can help increase the accuracy and reliability of the anomaly detection process by reducing false positives and false negatives. Figure 5.1 shows the precision of proposed system with existing system.

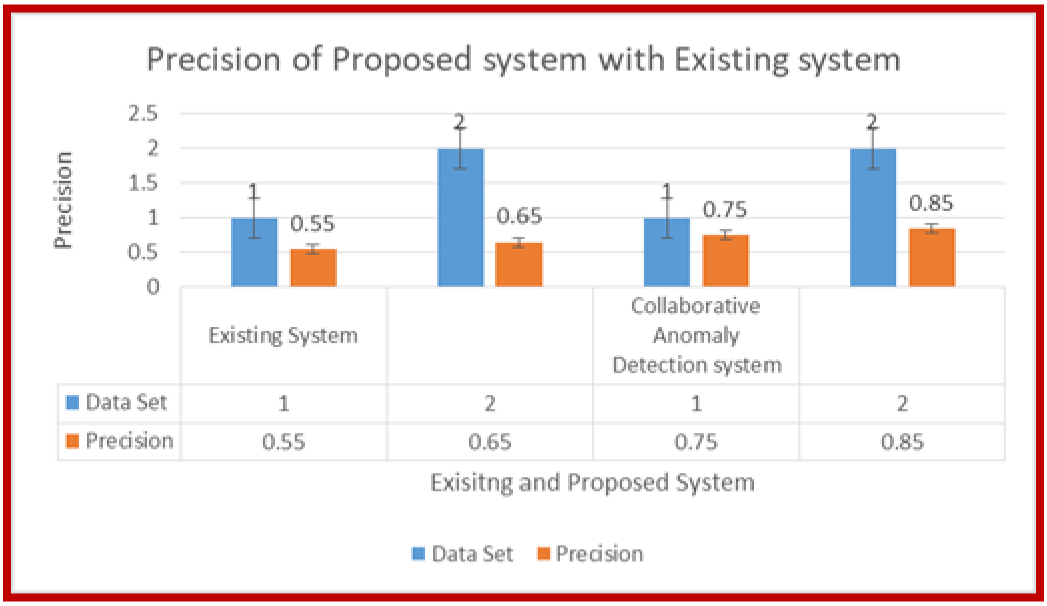

Figure 5.1: Precision of Collaborative Anomaly Detection system

The result of collaborative anomaly detection would be a list of data points deemed anomalous by the combination of the outputs from the different models or algorithms. These could be presented in a visual format or as a numerical score, depending on the particular implementation of the technique. Figure 5.2 shows the recall of proposed system with existing system.

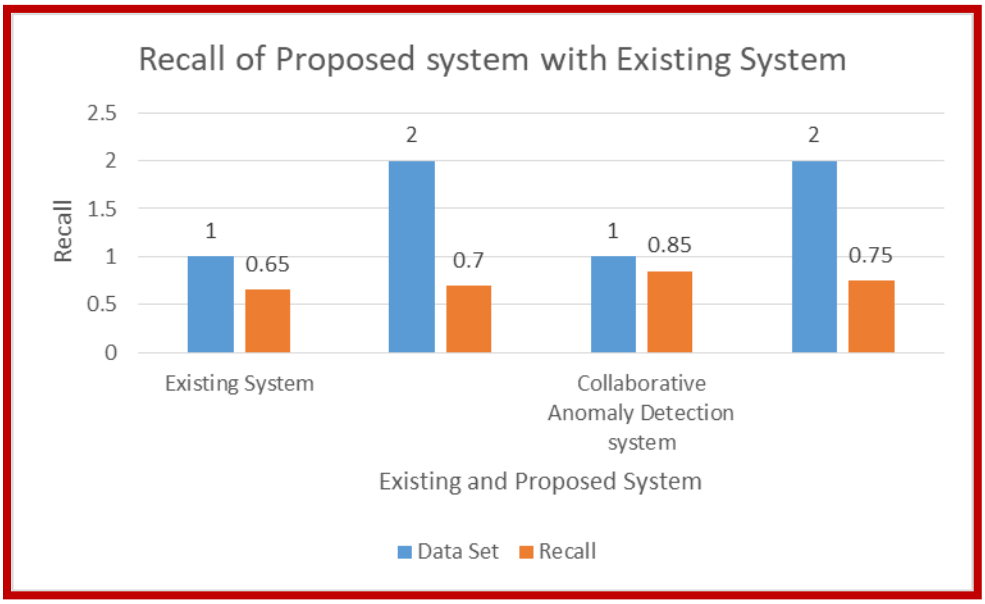

Figure 5.2: Recall of Collaborative Anomaly Detection system

An analysis of the results would involve examining the identified anomalies to determine their potential significance or impact, as well as evaluating the performance of the collaborative anomaly detection process as a whole. This could involve looking at metrics such as precision, recall, and F1 score to evaluate the accuracy and effectiveness of the technique in identifying true anomalies while minimizing false positives and false negatives. It could also involve examining the performance of the individual algorithms or models used in the collaborative process to determine their strengths and weaknesses.

6. Conclusion

6.1 Summary of the findings

Collaborative anomaly detection refers to a process in which multiple detection models or techniques are used in combination to identify anomalous behavior or events in a system. The goal of collaborative anomaly detection is to improve the accuracy and reliability of anomaly detection by leveraging the strengths of each technique and compensating for their weaknesses. Research studies have shown that collaborative anomaly detection can significantly improve the detection accuracy and reduce false positives when compared to individual techniques. The effectiveness of collaborative anomaly detection depends on the selection of appropriate techniques and the design of a suitable fusion rule for integrating the outputs of multiple models. One study compared the performance of different collaborative anomaly detection approaches on a real-world dataset and found that a simple voting rule for combining outputs from multiple models was effective in improving detection accuracy. Another study proposed a new approach called cascaded anomaly detection, which combined multiple models in a cascade structure that enabled early detection and reduced false positives. Collaborative anomaly detection has been applied in various domains, including network security, fraud detection, and medical diagnosis. In network security, multiple techniques such as rule-based, signature-based, and behavior-based detection are combined to detect various types of attacks. In fraud detection, multiple models are used to analyze different aspects of the data such as user behavior, transaction patterns, and social network relationships. In medical diagnosis, multiple diagnostic tests are used in combination to improve the accuracy of disease detection. Overall, collaborative anomaly detection has shown promise in improving the accuracy and reliability of anomaly detection in various domains. However, the selection and fusion of appropriate detection models remain a challenge, and further research is needed to develop effective collaborative anomaly detection techniques.

6.2 Implications and future research directions

Collaborative anomaly detection has promising implications for enhancing the accuracy, efficiency, and scalability of anomaly detection in various domains. Specifically, CAD enables multiple detectors to collaborate and exchange information to overcome the limitations of individual detectors and improve the overall detection performance. Some of the key implications and potential benefits of CAD include:

1. Increased detection accuracy: By collaborating and combining the results of several detectors, CAD can reduce false positives and false negatives, thereby improving the accuracy of anomaly detection.

2. Enhanced efficiency and scalability: CAD can distribute the detection workload across multiple detectors, reducing the processing time and enabling the detection of anomalies at a larger scale.

3. Improved adaptability and diversity: CAD can leverage diverse detectors with different strengths and weaknesses, enabling a more flexible and robust detection system that can adapt to different types of anomalies.

4. Better interpretability and explainability: CAD can provide insights into how various detectors contribute to the detection process and explain why certain anomalies are detected or missed.

Some of the possible future research directions for CAD include:

1. Developing more effective collaboration strategies: Existing CAD approaches mostly rely on simple combination methods, such as voting or averaging. Future research can explore more sophisticated strategies that take into account the diversity and reliability of different detectors.

2. Addressing privacy and security concerns: Collaborative anomaly detection involves sharing information among detectors, raising concerns about the privacy and security of sensitive data. Future research can explore privacy-preserving and secure CAD techniques that protect the privacy of data while enabling collaboration.

3. Integrating with other AI techniques: CAD can be integrated with other AI techniques, such as reinforcement learning, to improve the adaptability and autonomous decision-making capabilities of anomaly detectors.

4. Testing and validation in real-world applications: CAD has been mostly tested in controlled laboratory settings. Future research can investigate the effectiveness and practicality of CAD in real-world applications, such as cybersecurity, finance, and healthcare.

Overall, collaborative anomaly detection holds great potential for advancing the state-of-the-art in anomaly detection and providing more accurate and efficient detection systems.

References

[1] F. T. Liu, K. M. Ting and Z.-H. Zhou, "Isolation-based anomaly detection", *ACM Transactions on Knowledge Discovery from Data (TKDD)*, vol. 6, no. 1, pp. 3, 2012.

[2] Chandola, V., Banerjee, A., Kumar, V., 2009. Anomaly detection: A survey. ACM Comput. Surv. 41 (3), 1–58. http://dx.doi.org/10.1145/1541880.1541882.

[3] Ranshous, S., Shen, S., Koutra, D., Harenberg, S., Faloutsos, C. and Samatova, N.F. (2015), Anomaly detection in dynamic networks: a survey. WIREs Comput Stat, 7: 223-247. https://doi.org/10.1002/wics.1347

[4] Patcha A, Park J-M. An overview of anomaly detection techniques: existing solutions and latest technological trends. Comput Netw. 2007;51(12):3448–70.

[5] Oswal, S., Shinde, S., Vijayalakshmi, M. (2023). A Survey of Statistical, Machine Learning, and Deep Learning-Based Anomaly Detection Techniques for Time Series. In: Garg, D., Narayana, V.A., Suganthan, P.N., Anguera, J., Koppula, V.K., Gupta, S.K. (eds) Advanced Computing. IACC 2022. Communications in Computer and Information Science, vol 1782. Springer, Cham. https://doi.org/10.1007/978-3-031-35644-5_17

[6] Heard, Nicholas A., David J. Weston, Kiriaki Platanioti, and David J. Hand. “BAYESIAN ANOMALY DETECTION METHODS FOR SOCIAL NETWORKS.” The Annals of Applied Statistics 4, no. 2 (2010): 645–62. http://www.jstor.org/stable/29765524.

[7] Abdulla Amin Aburomman, Mamun Bin Ibne Reaz, A survey of intrusion detection systems based on ensemble and hybrid classifiers, Computers & Security, Volume 65, 2017, Pages 135-152, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2016.11.004.

[8] Max Landauer, Sebastian Onder, Florian Skopik, Markus Wurzenberger, Deep learning for anomaly detection in log data: A survey, Machine Learning with Applications, Volume 12, 2023, 100470, ISSN 2666-8270, https://doi.org/10.1016/j.mlwa.2023.100470.

[9] A. M. S. Ngo Bibinbe, M. F. Mbouopda, G. R. Mbiadou Saleu and E. Mephu Nguifo, "A survey on unsupervised learning algorithms for detecting abnormal points in streaming data," *2022 International Joint Conference on Neural Networks (IJCNN)*, Padua, Italy, 2022, pp. 1-8, doi: 10.1109/IJCNN55064.2022.9892195.

[10] Ranjeethapriya K, Susila N, Granty Regina Elwin, Balakrishnan S, “Raspberry Pi Based Intrusion Detection System”, International Journal of Pure and Applied Mathematics, Volume 119, No. 12, 2018, pp.1197-1205.

[11] S. Balakrishnan, B. Persis Urbana Ivy and S. Sudhakar Ilango, “A Novel And Secured Intrusion Detection System For Wireless Sensor Networks Using Identity Based Online/Offline Signature”, ARPN Journal of Engineering and Applied Sciences. November 2018, Vol. 13 No. 21, pp. 8544-8547.

[12] J.P.Ananth, S.Balakrishnan, S.P.Premnath, (2018). “Logo Based Pattern Matching Algorithm for Intrusion Detection System in Wireless Sensor Network”, International Journal of Pure and Applied Mathematics, Volume 119, No. 12, 2018, pp. 753-762.