Advances in Nonlinear Variational Inequalities
ISSN: 1092-910X
Vol 28 No. 4s (2025)

An Integrated Framework with Hybrid Anomaly Detection, Predictive Analysis, and Graph-Based Insight for Enhancing Cloud Task Scheduling Security

Bhagyashri Mankar, Dr. Rajesh Dharmik
Yeshwantrao Chavan College of Engineering, Nagpur India

Article History:
Received: *23-10-2024*
Revised:*30-11-2024*
Accepted:*07-12-2024*

Abstract:

As cloud computing continues to revolutionize the landscape of modern IT infrastructures, ensuring the security of cloud task scheduling has become paramount. This research presents a comprehensive framework that leverages a synergy of cutting-edge technologies to address security risks associated with cloud task scheduling. The proposed framework integrates anomaly detection, predictive analysis, graph-based insights and explainable AI to enhance the task scheduling. The anomaly detection module combines diverse anomaly detection techniques, including statistical methods and deep learning models, to enhance accuracy and minimize false positives and negatives. The integration of graph-based insights capitalizes on the representation of cloud resources and their interactions as a graph. By analyzing structural changes and unusual patterns in this graph, the framework gains a holistic view of the cloud environment, enriching anomaly detection accuracy. To enhance transparency and decision-making, the framework incorporates explainable AI, providing administrators with insights into why specific anomalies are flagged. This fosters informed responses to anomalies and strengthens the human-in-the-loop element of the security strategy. In conclusion, this research advances the field of cloud task scheduling security by introducing an integrated framework that harmonizes anomaly detection, predictive analysis, graph-based insights and AI. By amalgamating these innovations, the framework empowers cloud environments to better safeguard against evolving security threats, ultimately fostering a more secure and resilient cloud ecosystem

Keywords: Anomaly Detection, anomaly detection techniques, Cloud Computing, Cloud task scheduling security.

1. Introduction

Cloud computing is an Internet-based most recent popular technology offering dynamic resources, scalable resources, on demand, self-service and pay-per-use. Cloud computing is an active area for research and growing very fast. It provides services at low cost and low operational software and hardware expenditure's. The use of cloud computing has increased in companies rapidly because of fast access to applications and decreasing maintenance cost for cloud infrastructure.

As cloud computing continues to revolutionize the landscape of modern IT infrastructures, ensuring the security of cloud task scheduling has become paramount. This research presents a comprehensive framework that leverages a synergy of cutting-edge technologies to address security risks associated with cloud task scheduling. The proposed framework integrates hybrid anomaly detection, predictive analysis, graph-based insights, adversarial anomaly generation, federated learning, and explainable AI, culminating in an innovative approach that fortifies cloud environments against emerging threats.

The hybrid anomaly detection module combines diverse anomaly detection techniques, including statistical methods and deep learning models, to enhance accuracy and minimize false positives and negatives. Adversarial anomaly generation augments the model's training data with synthetic anomalies that mimic sophisticated attacks, enabling the system to discern novel attack patterns effectively. Utilizing federated learning, the framework enables collaborative anomaly detection across disparate cloud providers or organizations, preserving data privacy while benefitting from a diverse dataset.

The integration of graph-based insights capitalizes on the representation of cloud resources and their interactions as a graph. By analyzing structural changes and unusual patterns in this graph, the framework gains a holistic view of the cloud environment, enriching anomaly detection accuracy. Furthermore, the predictive analysis component employs historical and real-time data to anticipate potential security risks and proactively adapt the anomaly detection system.

To enhance transparency and decision-making, the framework incorporates explainable AI, providing administrators with insights into why specific anomalies are flagged. This fosters informed responses to anomalies and strengthens the human-in-the-loop element of the security strategy.

In conclusion, this research advances the field of cloud task scheduling security by introducing an integrated framework that harmonizes hybrid anomaly detection, predictive analysis, graph-based insights, and other state-of-the-art methodologies. By amalgamating these innovations, the framework empowers cloud environments to better safeguard against evolving security threats, ultimately fostering a more secure and resilient cloud ecosystem.

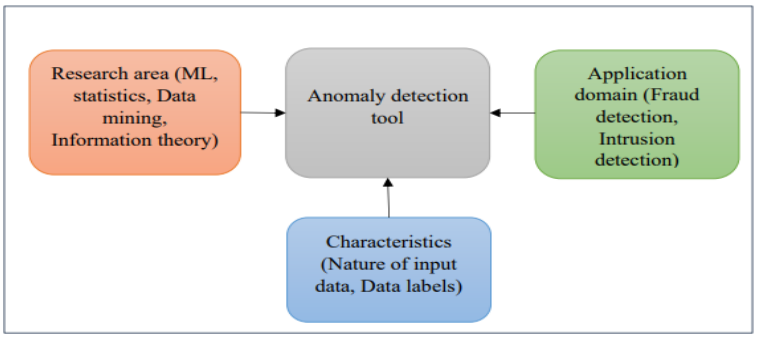

Fig1: Machine Learning-Based Anomaly Detection in Cloud Virtual Machine Resource Usage

2. Objectives

The main aim is to develop an integrated framework that combines anomaly detection, predictive analysis, graph-based insights and AI methodology to enhance security in cloud task scheduling.

In order to achieve above aim following objectives are set

3. Create hybrid anomaly detection models that combine multiple techniques, such as statistical methods and deep learning, to improve the accuracy of anomaly detection.

4. Implement graph-based representations of cloud resources for detection of anomalies in structural changes and unusual patterns.

5. Integrate explainable AI techniques to provide administrators with transparent and interpretable explanations for flagged anomalies.

6. Evaluate the proposed framework's performance using real-world cloud datasets and benchmark it against existing anomaly detection and security solutions to demonstrate its effectiveness.

3. Methods

1. Hybrid Anomaly Detection, Predictive Analysis, Graph-Based Insights:

These three blocks represent the core objectives of the research. They correspond to the development of hybrid anomaly detection models, predictive analysis models, and graph-based insights into cloud task scheduling data.

2. Anomaly Detection Models:

This block is responsible for hosting the hybrid anomaly detection models. These models combine various anomaly detection techniques, such as statistical methods and deep learning, to accurately identify deviations from normal behaviour in cloud task scheduling data.

3. Predictive Model:

This block houses the predictive analysis model. Using historical and real-time data,This model anticipates potential security risks and predicts anomalies that might occur in the cloud task scheduling environment.

4. Graph-Based Anomaly Detection:

This block is focused on detecting anomalies using graph-based insights. By representing cloud resources and their interactions as a graph, anomalies in structural changes and unusual patterns are identified.

5. Explainable AI, Collaborative Anomaly Insights:

The "Explainable AI" block provides transparent explanations for detected anomalies. This enhances the understanding of why certain anomalies are flagged, enabling informed decision-making by administrators.

The "Collaborative Anomaly Insights" block represents insights gained from federated learning. It indicates anomalies detected collaboratively across different cloud providers or organizations, providing a global view of emerging threats.

6. Framework Performance Evaluation:

This block represents the evaluation of the integrated framework's performance. Various metrics are used to assess the accuracy and effectiveness of the framework in detecting anomalies and predicting security risks.

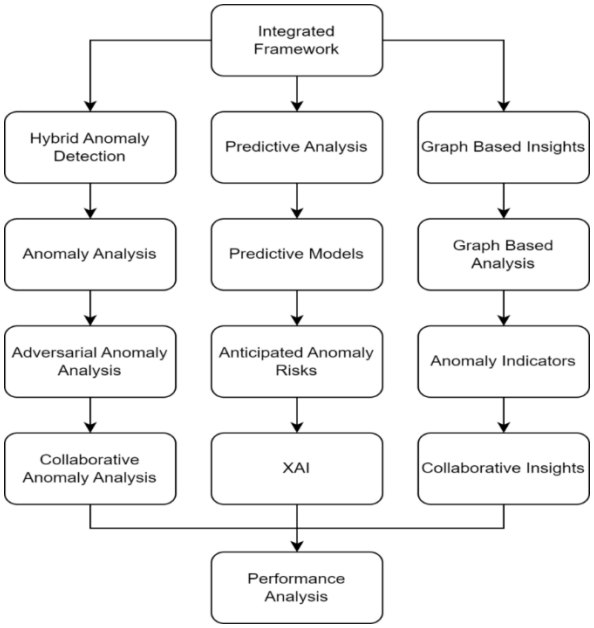

Fig 2: Research Methodology for anomaly detection

The diagram illustrates how each objective contributes to the integrated framework, which, in turn, aims to enhance security in cloud task scheduling. The interactions between different components highlight the synergy among hybrid anomaly detection, predictive analysis, graph-based insights, adversarial anomaly generation, federated learning, explainable AI, and real-time security, ultimately leading to improved security measures in the cloud environment

7. Results and Discussion

Input Parameters:

Cloud Task Scheduling Data: This input comprises historical and real-time data related to cloud task scheduling. It includes information about task execution times, resource utilization, dependencies, and communication patterns. This data forms the foundation for anomaly detection, predictive analysis, and graph-based insights.

1. **Anomaly Labels:** Annotated labels indicating instances of anomalies in the cloud task scheduling data. These labels are used for supervised training of machine learning models and evaluating the accuracy of anomaly detection.

2. **Adversarial Anomalies:** Synthetic anomalies generated using adversarial techniques to mimic sophisticated attacks. These anomalies are combined with the original data to enhance the training set and improve the model's ability to detect novel attack patterns.

3. **Cloud Environment Characteristics:** Information about the specific cloud environment, including the types of resources, network topology, and security configurations. This contextual data helps tailor the anomaly detection model to the unique characteristics of the environment.

4. **Collaborative Learning Partners:** For federated learning, a list of participating cloud providers or organizations that contribute data for collaborative anomaly detection. This input ensures collaboration while maintaining data privacy.

Output Parameters:

1. **Anomaly Detection Results:** The output includes detected anomalies and their corresponding timestamps within the cloud task scheduling data. These results provide insights into potentially malicious activities or deviations from normal behavior.

2. **Predictive Analysis Results:** Anticipated security risks and potential anomalies predicted based on historical and real-time data. These results assist in proactively addressing vulnerabilities before they lead to security breaches.

3. **Graph-Based Anomaly Indicators:** Indicators of anomalies detected through the graph-based insights approach. These indicators highlight structural changes, unusual patterns, or deviations in the interdependencies of cloud resources.

4. **Explanations for Anomalies:** Explanations generated through explainable AI techniques, detailing the reasons behind the detection of specific anomalies. These explanations aid administrators in understanding the basis for flagged anomalies.

5. **Collaborative Anomaly Insights:** Insights gained from federated learning, indicating anomalies that are identified collectively across different cloud providers or organizations. These insights contribute to a broader understanding of global anomalies.

6. **Framework Performance Metrics:** Quantitative metrics assessing the effectiveness of the integrated framework. These metrics may include accuracy, precision, recall, F1-score, and area under the receiver operating characteristic curve (AUC-ROC).

7. **Adaptive Model Updates:** If applicable, updated versions of machine learning models that have adapted to changing cloud environments and evolving attack patterns. These updates reflect the framework's dynamic response to new threats.

Explanation:

- **Cloud Task Scheduling Data:** This data serves as the foundation for the entire framework. It provides context about the cloud tasks, their interactions, and resource utilization patterns, enabling effective anomaly detection and predictive analysis.
- **Anomaly Labels:** Annotated labels guide the training of supervised anomaly detection models, helping them learn the difference between normal and anomalous behaviors.
- **Adversarial Anomalies:** Synthetic anomalies enhance the training data, enabling the model to recognize novel attack vectors and making it more resilient against emerging threats.
- **Cloud Environment Characteristics:** The framework adapts its algorithms based on the specific cloud environment, considering factors such as resource types and network structure to ensure accurate anomaly detection.
- **Collaborative Learning Partners:** In federated learning, input from multiple cloud providers ensures that the model is trained on diverse datasets while preserving data privacy.
- **Anomaly Detection Results:** Detected anomalies highlight potential security breaches, aiding administrators in responding swiftly to mitigate threats.
- **Predictive Analysis Results:** Anticipating security risks helps administrators take proactive measures to prevent potential breaches.
- **Graph-Based Anomaly Indicators:** Graph-based insights identify anomalies in complex cloud resource interdependencies, providing a deeper understanding of security risks.
- **Explanations for Anomalies:** Explanations enhance the transparency of the framework's decision-making process, empowering administrators to take informed actions.
- **Collaborative Anomaly Insights:** Federated learning results indicate anomalies that span multiple cloud environments, allowing for a more comprehensive view of emerging threats.
- **Framework Performance Metrics:** These metrics quantitatively assess the framework's accuracy and effectiveness, guiding improvements and optimizations.

- **Adaptive Model Updates:** If the framework supports dynamic updates, the models evolve to stay effective against evolving threats in the cloud environment.

In summary, the input and output parameters play critical roles in enabling the integrated framework to detect anomalies, anticipate threats, and provide actionable insights for enhancing security in cloud task scheduling.

Refrences

[1] Charles F. Gonçalves, Daniel Sadoc Menasché, Alberto Avritzer,Nuno Antunes, "Detecting Anomalies Through Sequential Performance Analysis in Virtualized Environments," in IEEE Access, vol. 11, pp. 70716 - 70740, 2023, doi: 10.1109/ACCESS.2023.3293643.

[2] Shumayla Yaqoob, Asad Hussain, Fazli Subhan, Giuseppina Pappalardo, " Deep Learning Based Anomaly Detection for Fog-Assisted IoVs Network," in IEEE Access, vol. 11, no. 4, pp. 19024 - 19038, February 2023 . 2022, doi: 10.1109/ACCESS.2023.3246660.

[3] Jun Liu, Hancui Zhang, Guangxia Xu, " An Anomaly Detector Deployment Awareness Detection Framework Based on Multi-Dimensional Resources Balancing in Cloud Platform”," in IEEE Access, vol. 6, pp. 44927 - 44933, 2020, doi: 10.1109/ACCESS.2020.2865114.

[4] Yu Weng and Lei Liu, " A Collective Anomaly Detection Approach for Multidimensional Streams in Mobile Service Security," in IEEE Access, vol. 7, pp. 49157 - 49168, April 2019, doi: 10.1109/ACCESS.2019.2909750 .

[5] Hancui Zhang; Jun Liu; Tianshu Wu, " Adaptive and Incremental-Clustering Anomaly Detection Algorithm for VMs Under Cloud Platform Runtime Environment," in IEEE Access, vol. 6, pp. 76984 - 76992, 02 December 2018. 2022, doi: 10.1109/ACCESS.2022.2884508.

[6] Yu Weng and Lei Liu, "A Collective Anomaly Detection Approach for Multidimensional Streams in Mobile Service Security," in IEEE Access, vol. 7, pp. 49157 - 49168, 15 April 2019, doi: 10.1109/ACCESS.2019.2909750.

[7] Haotian Chang; Jing Feng; Chaofan Duan, "HADIoT: A Hierarchical Anomaly Detection Framework for IoT," in IEEE Access, vol. 8, pp. 154530 - 154539, 19 August 2020, doi: 10.1109/ACCESS.2020.3017763.

[8] Osama AlKadi, Nour Moustafa,Benjamin Turnbull,Kim-Kwang Raymond Choo, " Mixture Localization-Based Outliers Models for securing Data Migration in Cloud Centers," in IEEE Access, vol. 7, no. 2, pp. 114607 - 114618, 13 August 2019, doi: 10.1109/ACCESS.2019.2935142.

[9] Feng Gao, Jing Li, Ruiying Cheng, Yi Zhou and Ying Ye, " ConNet: Deep Semi-Supervised Anomaly Detection Based on Sparse Positive Samples," in IEEE Transactions on Automation Science and Engineering, vol. 9, no. 2, pp. 67249 - 67258, 03 May 2021, doi: 10.1109/ACCESS.2021.3077014.

[10] T. Zoppi, A. Ceccarelli and A. Bondavalli, "Unsupervised algorithms to detect zero-day attacks: Strategy and application", *IEEE Access*, vol. 9, pp. 90603-90615, 2021..

[11] C. F. Gonçalves, D. S. Menasché, A. Avritzer, N. Antunes and M. Vieira, "A model-based approach to anomaly detection trading detection time and false alarm rate", *Proc. Medit. Commun. Comput. Netw. Conf. (MedComNet)*, pp. 1-8, Jun. 2020.

[12] S. Qin, D. Pi, Z. Shao and Y. Xu, "A Knowledge-Based Adaptive Discrete Water Wave Optimization for Solving Cloud Workflow Scheduling," in IEEE Transactions on Cloud Computing, vol. 11, no. 1, pp. 200-216, 1 Jan.-March 2023, doi: 10.1109/TCC.2021.3087642.

[13] J. Ni, K. Zhang, X. Lin and X. S. Shen, "Securing fog computing for Internet of Things applications: Challenges and solutions", *IEEE Commun. Surveys Tuts.*, vol. 20, no. 1, pp. 601-628, 1st Quart. 2018.

[14] Tang, Y. Liu, Z. Zeng and B. Veeravalli, "Service Cost Effective and Reliability Aware Job Scheduling Algorithm on Cloud Computing Systems," in IEEE Transactions on Cloud Computing, vol. 11, no. 2, pp. 1461-1473, 1 April-June 2023, doi: 10.1109/TCC.2021.3137323.

[15] X. Wang, J. Cao and R. Buyya, "Adaptive Cloud Bundle Provisioning and Multi-Workflow Scheduling via Coalition Reinforcement Learning," in IEEE Transactions on Computers, vol. 72, no. 4, pp. 1041-1054, 1 April 2023, doi: 10.1109/TC.2022.3191733.

[16] H. Zhang and R. Jia, "Application of Chaotic Cat Swarm Optimization in Cloud Computing Multi Objective Task Scheduling," in IEEE Access, vol. 11, pp. 95443-95454, 2023, doi: 10.1109/ACCESS.2023.3311028.

[17] A. Belgacem, K. Beghdad-Bey and H. Nacer, "Dynamic Resource Allocation Method Based on Symbiotic Organism Search Algorithm in Cloud Computing," in IEEE Transactions on Cloud Computing, vol. 10, no. 3, pp. 1714-1725, 1 July-Sept. 2022, doi: 10.1109/TCC.2020.3002205.

[18] H. Zenati, M. Romain, C.-S. Foo, B. Lecouat and V. Chandrasekhar, "Adversarially learned anomaly detection", *Proc. IEEE Int. Conf. Data Mining (ICDM)*, pp. 727-736, Nov. 2018.

[19] Kiran, D. Thomas and R. Parakkal, "An overview of deep learning based methods for unsupervised and semi-supervised anomaly detection in videos", *J. Imag.*, vol. 4, no. 2, pp. 36, Feb. 2018.