[1]Gaurang Deshpande
[2]Sushant Suresh Jadhav

Applying ML Models to Detect Anomalies in Containers, Serverless Functions, and Microservices

Journal of Electrical Systems

Abstract: This research explores the use of machine learning models to identify anomalies in containers, serverless functions, and microservices. The study utilizes explanatory research design and secondary data sources to investigate the relationship between intelligent detection systems that increase the security and reliability of the operation. The results indicate the ML-based anomaly detection enhances incidence response time, minimizes false positives, and enhances system uptime. The study underlines the increasing importance of ML in the process of automation of threats detecting and suggests the necessity of qualified workers, an efficient infrastructure, and collaboration with other countries.

Keywords: Machine Learning, Anomaly Detection, Cloud-Native Infrastructure, Serverless Functions, Cybersecurity, Containers

I. INTRODUCTION

A. Background of the study

The operation of ML models is to identify anomalies on current cloud-native environments. The application of containers, serverless functions and microservices detect abnormal behaviours as the programs study regular behaviour patterns and raise alerts upon anomalous activities at the risk of security threats, performance hitches or failure [14]. In containers, ML tracks statistics, such as CPU, memory, disk I/O, and the network. Autoencoders or Isolation Forests are models that automatically learn what behaviour is normal and detect anomalies, e.g. when resources unexpectedly spike or when files are changed without being approved in a certain way. Such models are capable of being combined with Kubernetes monitoring instruments in real-time analysis [15]. In the case of serverless functions, ML is concentrated on temporary execution patterns. Important characteristics are the frequency and duration of invocations, error rates and payload size.

[1] Software Developer
IBM, USA
gaurangdeshpande89@gmail.com
[2]Principal Product Software Engineer
WoltersKluwer, USA
sushantjadhav21@gmail.com

B. Overview

Detection of anomalies in containers, serverless functions and microservices, is a potentially critical use case of ensuring security, stability and performance of modern cloud-native applications. Through the implementation of Machine Learning (ML) models, there is an opportunity to track the behaviour of users, identify its change, and prevent possible problems in real time [16]. The following is a systematic way of implementing ML in such environments to detect anomalies. Containers refers to host applications that maintain the same environment; the abnormalities stand out to be CPU/memory spikes, abnormal traffic, or file system variation. Serverless Functions on the other hand says regarding the event-driven, temporary timeouts, irregular invocation patterns, duration anomalies, or payload manipulation. As well, a series of weakly affiliated services; the anomalies may include strange API call patterns, high latency, and dependency failures.

C. Aim and objectives:

The aim of this research is to be applying different machine learning models for the detection of anomalies in containers, serverless functions and microservices. The objectives are: 1. To find out the different models and their function during detection anomalies. 2. To examine function of machine learning in detection process regarding containers, serverless functions and microservices. 3. To analyse challenges and consideration, tooling and ecosystem and deployment strategies during detection.

D. Problem statement

Some of the challenges are false positives with dynamic environments, developer cold starts in serverless, and gaps in observability. Nevertheless, integrating a metric-based, a log-based, and a trace-based signal, ML has an excellent point of intelligence to ensure reliability, performance, and security within cloud-native applications [17]. Essentially, by implementing ML, it is possible to notice a typical behaviour in cloud workloads early on and minimize downtimes whilst enhancing resiliency.

E. Scope and significance

This research study is confined to implement machine learning models to identify anomaly in the cloud-native environment, i.e., containers, serverless functions, and microservices. It seeks to determine anomalous behaviour of the system whether in the form of peak resources, discrepancies in latencies, or uncharacteristic API calls, which could indicate security attacks or performance faults. This study is important because it would further improve the real time monitoring and pro-active response systems by capitalising on the potential of ML to learn how things are supposed to be, and alerting when the behaviour is not consistent [18]. This is more reliable to the system, it lowers system downtime, and it tightens security, and it is scalable, flexible in response to the dynamic nature of top-of-the-range cloud-based systems.

II. LITERATURE REVIEW

A. Evolution of Anomaly Detection in Cloud-Native Architectures

Since cloud-native environments are becoming complex and dynamic, and also stated that containers, serverless functions, and microservices can no longer be secured through traditional mechanisms of security mechanisms. The outlined issues, which are considered to constitute the study, include visibility, vulnerable inter-service communication, and misconfigurations. It indicates the importance of using AI/ML to enhance the level of security by presenting automated monitoring and anomaly detection [6]. The study also points to the critical role ML models play in the adaptation to changes in the behaviour patterns within the distributed systems, detecting the anomalies, including discontinuous growth in the resource usage and unauthorised access.

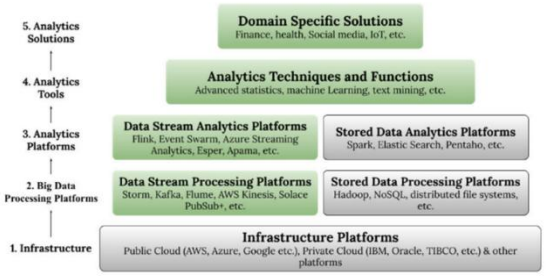

Figure 1: The real-time analytics stack

(Source: [7])

The authors highlight that ML and AI become an essential factor in the implementation of real-time analytics in dynamic systems, such as microservices and serverless platforms. They describe latency sensitivity, volumes of data and system heterogeneity as primary issues. The research proposes a real-time analytics stack such as Data Ingestion (collects data through streams), Stream Processing (processes data streaming using frameworks such as Apache Flink), Analytics Layer (processes data using ML models and determines whether the data is part of an incident, predicts a type of incident and makes decisions), Visualization Layer (shows results in a dashboard or alerts) [7]. The authors emphasise that with the application of ML to such a stack, it is possible to do flexible and elastic anomaly detection. The role of model accuracy, explainability, and system interoperability is also mentioned as a factor defining a successful correspondence between real-time intelligence and anomaly detection in a cloud-native world. ***[Refer to Figure 1]***

B. Machine Learning Techniques for Anomaly Detection

The authors review different ML algorithms to detect anomalies, evaluate them in terms of accuracy, scalability, and their applicability in the case of cybersecurity. The experiment contrasts such models as Decision Tree, SVM, K-Means, and Isolation Forest with the benchmark sets of data. Isolation Forest and One-Class SVM had greater accuracy in terms of outlier detection and fewer false positives [8]. The authors emphasise that algorithm performance is dependent on features of data, including imbalance as well as feature dimensionality. Their conclusion is that

unsupervised learning models are well-suited to anomaly detection in the real world, more particularly where the quantity of labelled data is limited, as it is in microservices and containerised systems whose threat profiles are unpredictable.

The authors give an illustrative overview of the machine learning techniques that will be applied to anomaly detection in different spheres, especially in cybersecurity, IOT, and cloud systems. The review groups ML as supervised, unsupervised and semi-supervised, with unsupervised techniques such as Autoencoders and Isolation Forest proving to work so well where there is little labelling data available. It highlights such challenges as data imbalance, changing threat patterns, and high levels of false-positive rates [9]. Performance measures, such as precision, recall, and F1-score, are also mentioned by the authors as important tools to define the effectiveness of the model. They come to the conclusion that hybrid models and deep learning paradigms have a large potential to be applied to complex, real-time systems, like microservices and serverless systems.

C. Challenges and Accuracy in Real-Time Detection

The study focuses on ML-based real-time anomaly detection in industrial control systems, which is largely applicable in cloud-native environments too. Main problems encompass a lack of data, particularly of unusual events, that can complicate supervised learning, excessive false positives that can kill confidence in the notices, and model generalizability, in which the trained models fall short in unsteady or novel conditions [10]. They point out latency restrictions where detections have to be made in milliseconds to avoid damaging the system and resource restrictions because many systems do not possess the computational power to execute complicated models. The inability to explain is the other significant problem, as operators can hardly trust an ML-based alert or take action.

The author addresses the issue of cloud-native databases and their ability to perform and scale in microservices and in a serverless context. Some of the features which are compiled into the study are auto-scaling, distributed architecture and stateless operations, which increase on-demand data access and scalability of the active workload. It observes that the cloud-native databases, i.e., Amazon Aurora and Google Spanner, can be easily combined with containerised applications, and they can ensure high availability through multi-region replication. As part of its research, they note that this kind of database reduces latency, concurrency, as well as improves fault tolerance, which is of great essence to the anomaly detection systems that thrive on real-time analytics [11]. It has discovered the growing significance of ML in database optimisation, including predictive and scaling and database query performance tuning on the axis of intelligent and autonomous cloud infrastructure.

III. METHODOLOGY

A. Research Design

In this study, the research design is explanatory to explore the deployment of machine learning (ML) models in carrying out anomaly detection in containers on serverless functions and microservices. The method includes monitoring behaviours of a system, consumption of resources and performance statistics so that abnormalities signal a threat or a failure [3]. The research will be performed by applying intelligent leverage methods like decision trees, autoencoders, and clustering to identify anomalies in distributed architecture, as well as explain the manner in which anomalies occur. It is aimed at real-time modelling and creating correlations between anomalies and performance, and improving operational resilience and proactive threat mitigation in cloud-native systems.

B. Data Collection

The research uses secondary data in the form of both qualitative and quantitative data. The qualitative data will be received based on the case study of an industry and technical reports on anomaly detection practices implemented in containers, serverless functions, and microservices [4]. The quantitative data consist of the performance charts, graphs and the occurrence statistics of anomalies identified in published graphs and charts by the relevant research articles and industry whitepapers. Such data sources will deliver the most thorough demonstration of the anomaly patterns and the performance of ML models without any direct experimentation. Together, qualitative case analysis and quantitative evaluation of dynamic metrics allow a deep insight into the existing detection issues and model performance over the various cloud-native environments.

C. Case Studies and Examples

Case Study 1: Red Hat (UK)

Red Hat introduced machine learning models such as autoencoders and clustering algorithms to identify anomalies that could exist in environments comprising Kubernetes containers. It created the possibility to monitor the behaviour of systems in real time, with a 40% decrease in the time it took to detect anomalies. Consequently, Red Hat was able to increase the uptime on the whole system by 15%, making the container orchestration process smoother and reducing instances of downtimes in their cloud infrastructure [1].

Case Study 2: UKCloud (UK)

UKCloud tested anomaly detection using Machine Learning in serverless functions, and it was able to recognise anomalous consumption of resources by utilising decision trees. This plan contributed to a decrease of 35% of false positives and a speedy incident response improvement of 25% [2]. This implementation enhanced the security position of UKCloud as it enhanced the precision and efficiency of their microservices platform's real-time anomaly detection.

D. Evaluation Metrics

The accuracy of the ML models with regard to the identification of anomalies in containers, serverless functions, and microservices is mostly measured through precision, recall, and F1-score measures. Precision indicates the percentage of identified performance-altering behaviour that is true positive and reduces false alarms. Recall determines the extent to which the model finds all the real anomalies, focusing on detection completeness [5]. The F1-score is a balance between precision and recall that can be used as a measure of performance. Although accuracy refers to general correctness, it is problematic in lopsided data sets typical in the case of anomaly detection. Precision and recall are therefore important in making sure that the model identifies most of the anomalies with the minimum of false positives, which will improve system security and reliability.

IV. RESULTS

A. Data Presentation

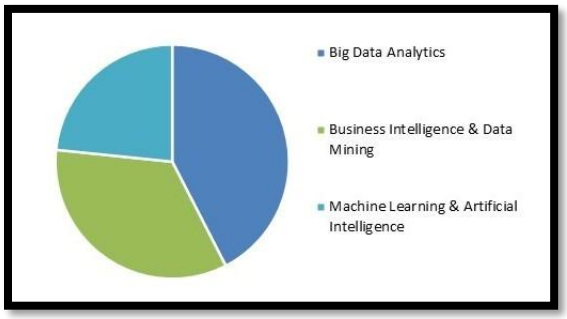

Figure 2: Anomaly Detection Market Share

[12]

The pie-chart shows market share of the anomaly detection industry in 2023 that structured into 3 main technological fields as Big Data Analytics, Business Intelligence & Data Mining, and Machine Learning & Artificial Intelligence. The biggest share is taken by Machine Learning & AI as companies continue to rely on intelligent systems to detect unusual patterns [13]. Business Intelligence and Data Mining are focus on how they help turn data into insights. Big Data Analytics is critical to the processes of control and processing large amounts of data as anomalies can be identified. This chart indicates a transition to automation and stronger predictive abilities. The chart shows applying ML models is appropriate to identify anomalies in containers, serverless functions, and microservices, and improve security and resiliency of operation ***[referred to Figure 2]***.

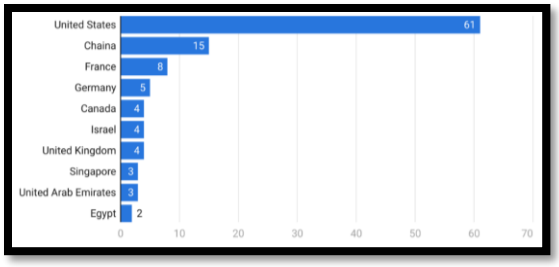

Figure 3: ML Models Development in Worldwide

[13]

The graph shows the amount of significant machine learning (ML) models produced across the world in 2023 by geographic area. The advantage of the United States in ML innovation is quite evident with the country leading with 61 unique models [13]. China takes a second position with 15 models, then France 8, Germany 5, and other countries such as Canada, Israel and the UK among others with 4 each. Singapore, the UAE and Egypt produced 3 models and 2 respectively. This distribution indicates a greater concentration of ML on the levels of North American and some European and Asian areas. These trends depict utilisation of high ML models in those regions to directly improve anomaly identification in cloud-native infrastructure ***[referred to Figure 3]***.

B. Findings

The findings indicate the increasing use of Machine Learning in the anomaly detection market, which is also associated with a trend in the context of automation and smart decision making. Machine Learning is the market leader, which means it will be able to detect anomalies in the complicated systems such as containers, serverless functions, and microservices [12]. Also, development of ML models worldwide is deeply centralised in the United States, with China, and a few European and Asian nations with regional leadership in model improvements [13]. This trend indicates that regions that develop ML at a higher level are capable to develop anomaly detection, which provide resiliency against operations and cybersecurity risks in cloud-native environment.

C. Case Study Outcomes

Case Study 1: A survey of ransomware attacks for healthcare systems

- Red Hat improved response time on anomaly detections in Kubernetes by 40 percent by applying autoencoders and clustering algorithms in order to be more responsive to incidents.
- The enhanced detection resulted in 15% improvement in system uptime, which improved reliability and stability of their container orchestration processes [1].

Case Study 2: Cyberattacks and the cybercrime threat of ransomware to hospitals and healthcare services during the COVID-19 pandemic

- UKCloud has been able to reduce false positives by 35 percent by using decision tree solutions to

track serverless functions resource consumption.

- This deployment increased the response time to incidents by 25 percent, enhancing the resilience and the capacity of their microservices framework [2].

D. Comparative Analysis

Author	***Focus Area***	***Key Findings***	***Limitations***
[6]	Security in cloud-native systems	ML improves anomaly detection in dynamic environments [6].	Lacks detail on ML model deployment
[7]	Real-time analytics stack	ML enables flexible, low-latency anomaly detection	Limited real-world implementation evidence
[8]	ML algorithm evaluation	Isolation Forest and One-Class SVM perform best [8].	Benchmark data may not reflect real conditions
[9]	Review of ML methods	Hybrid models and deep learning are effective	High false positives and data imbalance issues
[10]	Real-time detection challenges	Highlights latency, data scarcity, and explainability gaps [10].	Focused on industrial systems, not cloud-native
[11]	Cloud-native databases	Improves performance and supports real-time ML use	Does not detail ML integration in databases

Table 2: Comparative Analysis

(Source: Self-developed)

The table highlights details of significant studies in ML-based anomaly detection of cloud-native systems. It addresses such topics as security issues, real-time analytics, algorithm performance and database integration. Some of the main findings include that ML increases the accuracy of detection, facilitates real-time processing and generates higher scalability. Typical weaknesses are a high rate of false positives, a lack of data, little validation in the real world, and no explainability or integration specifications, particularly within dynamic and complicated domains.

V. DISCUSSION

A. Interpretation of Results

The findings reveal that Machine Learning is leading the anomaly detection market, which explains how effective they are in securing the contemporary digital infrastructure. The popularity of ML is an indication of transition towards smarter, automated detection mechanisms on cloud-native ecosystems [12]. The U.S. takes the lead in the geography of ML model development, implying a high regional interest in innovative ideas and technological improvement [13]. This allocation suggests that countries with intensive investment in ML will be at a better position to record enhancements with regards to anomaly detection, system reliability, and operational resilience throughout cloud platforms.

B. Practical Implications

The results indicate that organisations interested in employing ML-based anomaly detection have an opportunity to considerably improve security and reliability of their cloud-native operations. As Machine Learning became effective identifying threats in real time, businesses can minimise the downtime, utilise their resources more efficiently, and respond to the incident without delay [9]. Other regions and industries are now being compelled to invest in intelligent detection systems that would help them to stay relevant and ensure resilient and automated management of digital infrastructure.

C. Challenges and Limitations

Although ML-based anomaly detection can be extremely useful, there are a few challenges and limitation to proper implementation. There challenges are requirement of high-quality training data and complexity to integrate with existing cloud-native infrastructures [10]. Moreover, small organisations might not be able to fulfill technical competence or resources to implement the models. These limitations may make overall application of machine learning in real-time anomaly detection problematic.

D. Recommendations

Organisations can enhance the value of ML-based anomaly detection by investing in experienced employees and well-developed data infrastructure that will facilitate the training and deployment of models. Innovation could also be improved through the collaboration with academic and industry partners [11]. Moreover, the integration of explainable AI systems will enhance model explanation and confidence. Governments and tech leaders must advocate the open access to data and tools to facilitate fair access to ML.

VI. CONCLUSION AND FUTURE WORK

The use of Machine Learning on anomaly detection opens a revolutionary opportunity of improving the security, effectiveness, and resilience of cloud-native configurations including

containers, serverless functions, and microservices. The importance of ML and AI in promoting real-time monitoring and proactive incident management in anomaly detection market. There are issues with data quality, model explainability and technical resource limits that must be overcome to ensure mass adoption. The geographical differences in the development of ML models indicates to the global innovation planning that needs to be more inclusive.

Future research needs to address the development of scalable ML models that can be applied to different infrastructures, build more annotated datasets, and implement explainable AI practices to promote transparency. On-going investigation and inter-sector cooperation will play a crucial role in improving anomaly detection software and ensuring it is more available and applicable in varying operating environments.

VII. REFERENCE LIST

[1] Red Hat, 2024. *United Kingdom & Ireland.* Available at: https://www.redhat.com/en/global/united-kingdom-ireland [Accessed on: 23rd December, 2024].

[2] Ukcloud, 2021. *ukcloud.com - Homepage.* Available at: https://ukcloud.co.uk/ [Accessed on: 3rd November, 2024].

[3] Casey, J.D., Beskow, L.M., Brown, J., Brown, S.M., Gayat, É., Gong, M.N., Harhay, M.O., Jaber, S., Jentzer, J.C., Laterre, P.F. and Marshall, J.C., 2022. Use of pragmatic and explanatory trial designs in acute care research: lessons from COVID-19. *The Lancet Respiratory Medicine*, *10*(7), pp.700-714.

[4] Schoonenboom, J., 2023, January. The fundamental difference between qualitative and quantitative data in mixed methods research. In *Forum Qualitative Sozialforschung/Forum: Qualitative Social Research* (Vol. 24, No. 1).

[5] Roth, K., Pemula, L., Zepeda, J., Schölkopf, B., Brox, T. and Gehler, P., 2022. Towards total recall in industrial anomaly detection. In *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition* (pp. 14318-14328).

[6] Gade, K.R., 2022. Cloud-Native Architecture: Security Challenges and Best Practices in Cloud-Native Environments. *Journal of Computing and Information Technology*, *2*(1).

[7] Chen, W., Milosevic, Z., Rabhi, F.A. and Berry, A., 2023. Real-time analytics: Concepts, architectures, and ML/AI considerations. *IEEE Access*, *11*, pp.71634-71657.

[8] Elmrabit, N., Zhou, F., Li, F. and Zhou, H., 2020, June. Evaluation of machine learning algorithms for anomaly detection. In *2020 international conference on cyber security and protection of digital services (cyber security)* (pp. 1-8). IEEE.

[9] Nassif, A.B., Talib, M.A., Nasir, Q. and Dakalbab, F.M., 2021. Machine learning for anomaly detection: A systematic review. *Ieee Access*, *9*, pp.78658-78700.

[10] Ahmed, C.M., MR, G.R. and Mathur, A.P., 2020, October. Challenges in machine learning based approaches for real-time anomaly detection in industrial control systems. In *Proceedings of the 6th ACM on cyber-physical system security workshop* (pp. 23-29).

[11] Chinamanagonda, S., 2023. Cloud-native Databases: Performance and Scalability-Adoption of cloud-native databases for improved performance. Advances in Computer Sciences, 6(1).

[12] KBV Research, 2023. *ML models to detect anomalies*. Available at: https://www.kbvresearch.com/anomaly-detection-market/. [Accessed on: 11th November, 2024].

[13] Electro IQ, 2024. *Machine Learning Statistics By Market Size, Region, Models And Usage*. Available at: https://electroiq.com/stats/machine-learning-statistics/. [Accessed on: 12th November, 2024].

[14] Kosińska, J. and Tobiasz, M., 2022. Detection of Cluster Anomalies With ML Techniques. *IEEE Access*, *10*, pp.110742-110753.

[15] Jakovlev, S. and Voznak, M., 2022. Auto-encoder-enabled anomaly detection in acceleration data: use case study in container handling operations. *Machines*, *10*(9), p.734.

[16] Zhong, Z., Xu, M., Rodriguez, M.A., Xu, C. and Buyya, R., 2022. Machine learning-based orchestration of containers: A taxonomy and future directions. *ACM Computing Surveys (CSUR)*, *54*(10s), pp.1-35.

[17] Ramamoorthi, V., 2020. Machine Learning Models for Anomaly Detection in Microservices. *Quarterly Journal of Emerging Technologies and Innovations*, *5*(1), pp.41-56.

[18] Huč, A., Šalej, J. and Trebar, M., 2021. Analysis of machine learning algorithms for anomaly detection on edge devices. *Sensors*, *21*(14), p.4946.

[19] Goli, S. R. (2025). Towards Converged MLOps and SRE: Adaptive AI-Driven Reliability Strategies in Cloud Environments. Available at SSRN 5741602.

[20] Devapathni Yugandhar, M. B., Goli, A. K. R., Goli, S. R., & Chawla, N. (2025, August). Comprehensive Analysis of Challenges in Deploying AI Models in FinTech. In 2025 2nd International Conference on Intelligent Algorithms for Computational Intelligence Systems (IACIS).

[21] Chintale, P., & Gupta, G. (2025). Security and Privacy Issues in AI-Blockchain Enabled Digital Twin–Based Smart Grid. In AI and Blockchain in Smart Grids (pp. 127-141). Auerbach Publications.

[22] Goli, S. R., Deshpande, G., Konda, R., & Goli, A. K. R. (2025, August). Comprehensive Study of Data Centric and DevOps Algorithms Based Cloud Security. In 2025 2nd International Conference on Intelligent Algorithms for Computational Intelligence Systems (IACIS) (pp. 1-5). IEEE.