Economic, Management, Business and Accountancy International Journal,
2 (2) 2025, 74-78
ECONOMIC, MANAGEMENT, BUSINESS AND ACCOUNTANCY INTERNATIONAL JOURNAL
https://journal.mjkpublisher.or.id/index.php/EMBAIJ

Application of FinOps-Based Cloud Cost Risk Analysis on Microsoft Azure Services

Dzihni Safwa Alifah[1], Mahadika Rastia Wardana[2], Yulia Cahyani[3], Ilham Albana[4]
[1,2,3,4] *Universitas Amikom Purwokerto, Indonesia*

Article Info

Article history:
Received: 10 October 2025;
Accepted: 20 November 2025;
Published: December 2025.

Keywords: Azure; Cloud computing; FinOps; Z-Score

Abstract

The increasing adoption of cloud computing simplifies IT infrastructure management but also introduces challenges related to unpredictable cost fluctuations. This study applies a descriptive quantitative approach using the Z-Score method to detect cloud cost anomalies as an initial step in FinOps practices. Microsoft Azure service cost data from the 2023–2024 period were analyzed through data cleansing, statistical calculations, and cost trend visualization. Using a Z-Score threshold of ≥ 1.7, the results indicate that one month was identified as High Risk with a Z-Score value of 2.275, representing a significant cost spike. These findings demonstrate that the Z-Score method is capable of detecting cost deviations quickly and efficiently without requiring complex analytical models, making it effective as an early warning system prior to the adoption of more advanced analytics techniques.

Abstrak

Penggunaan platform komputasi berbasis internet yang semakin luas memudahkan pengelolaan infrastruktur TI, namun juga menimbulkan tantangan berupa fluktuasi biaya yang sulit diprediksi. Penelitian ini menerapkan pendekatan kuantitatif deskriptif menggunakan metode Z-Score untuk mendeteksi pemyimpangan biaya layanan sebagai langkah awal praktik FinOps. Data biaya layanan Microsoft Azure periode 2023–2024 dianalisis melalui tahapan pembersihan data, perhitungan statistik, dan visualisasi tren biaya. Dengan ambang batas Z-Score ≥ 1,7, hasil menunjukkan satu bulan teridentifikasi sebagai risiko tertinggi dengan nilai Z-Score 2,275, yang mengindikasikan lonjakan biaya signifikan. Temuan ini menunjukkan bahwa Z-Score mampu mendeteksi penyimpangan biaya secara cepat dan efisien tanpa memerlukan model kompleks, sehingga efektif sebagai sistem peringatan dini sebelum organisasi mengadopsi metode analisis yang lebih canggih.

How to Cite:
Alifah, D.S., Wardana, M.R., Cahyani, Y., & Albana, I. (2025). Application of FinOps-Based Cloud Cost Risk Analysis on Microsoft Azure Services. *Economic, Management, Business and Accountancy International Journal*, 2(2), 74-78. https://doi.org/10.21009/EMBAIJ.002.2.5

* Corresponding Author.
dzihnisafwaa@gmail.com. Dzihni Safwa Alifah

ISSN
3110-6366 (online) DOI:
doi.org/10.21009/EMBAIJ.002.2.5

INTRODUCTION

Advancements in cloud computing technology have enabled organizations to manage their systems more flexibly and efficiently. Service models such as Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) have become primary choices across various industries to optimize information technology operations. However, alongside these benefits, new challenges emerge in controlling and predicting cloud costs, which often fluctuate significantly, particularly when service usage increases unexpectedly. This condition introduces financial risks in the form of cost spikes that are difficult to detect through manual monitoring.

Financial Operations (FinOps) has emerged as a collaborative practice that integrates technical, financial, and managerial teams to optimize cloud costs through transparency and controlled resource utilization. One of the critical initial steps in FinOps implementation is early detection of cloud cost anomalies, which may indicate service misconfigurations or inefficient resource usage.

Previous studies indicate that cloud anomaly detection commonly relies on machine learning and deep learning techniques. (Islam et al., 2020) identified key challenges in large-scale cloud anomaly detection, including high-dimensional telemetry data and the need for high-throughput multivariate processing. Their evaluation showed that both supervised and unsupervised learning approaches are effective in detecting abnormal usage patterns. Similarly, a systematic review by (Katsarou, 2020) highlighted the superiority of deep learning in handling large-scale non-linear data due to its advanced feature extraction capabilities. However, the study also emphasized practical limitations such as high computational costs, extensive training data requirements, and implementation complexity.

Meanwhile, (Yakkanti, 2025) emphasized that many organizations are still in the early stages of FinOps adoption and require gradual approaches to cloud cost management. Although AI-based solutions can automate cost monitoring and optimization recommendations, organizations still need simple and lightweight methods capable of providing early warnings without imposing high computational overhead. This creates a research gap regarding the need for efficient, practical, and low-resource anomaly detection methods, particularly during the early phase of FinOps implementation.

Therefore, this study proposes the use of the Z-Score statistical method as a lightweight and easily implementable solution for detecting cost anomalies in Microsoft Azure services.

LITERATURE REVIEW

1. Azure

Microsoft Azure is a full-featured public cloud platform offering services for compute, storage, and networking, managing IaaS, PaaS, and SaaS layers. Azure provides built-in cost management and governance tools that allow organizations to track consumption, set budgets, and set alerts. A study by (Bhardwaj, 2021) examining Azure costs emphasized the role of telemetry (billing records, resource tags, and telemetry logs) as a foundation for right-sizing. The study showed that Azure-specific tools can be integrated into FinOps workflows to provide near-real-time visibility and automated remediation for common cost leakage scenarios.

2. Cloud Computing

Microsoft Cloud computing is the provision of on-demand resources over the internet, typically delivered through services such as IaaS, PaaS, and SaaS. Literature since 2020 has repeatedly highlighted its benefits, including scalability, agility, and cost flexibility, while documenting challenges such as cost uncertainty, security, and governance. (Aljanabi et al., 2021) examines advances in cloud architecture, QoS issues, and operational challenges as organizations migrate complex workloads. The survey also underscores the need for a framework to monitor integrated governance.

3. FinOps

A cross-functional practice called FinOps involves engineering, finance, and business teams working together to manage cloud spending through collective accountability, real-time visibility, and continuous optimization. A recent practitioner study (2020–2024) described FinOps as a cultural practice and a range of operational processes: establishing cost allocations and showbacks/chargebacks, adopting reservation and savings plans, and embedding automated safeguards and alerts into CI/CD pipelines. (Sikha & Siramgari, 2023) stated that FinOps accelerates cloud adoption by making cost behavior visible to decision-makers and enabling them to

Alifah, D.S., Wardana, M.R., Cahyani, Y., & Albana, I. *Economic, Management, Business and Accountancy International Journal*, 2 (2) 2025, 74-78

ISSN 3110-6366 (online) DOI: doi.org/10.21009/EMBAIJ.002.2.5

consider better options for cost reduction. However, some studies caution that mature FinOps operations often require cultural change, standardization of tagging and telemetry, and integration of tools for scale.

4. Z-Score

Z-score-based rules are widely used in the anomaly detection literature as a simple and easy-to-understand detector for univariate time series, such as daily or monthly cost aggregates. Standardized scores are a simple statistical method used to calculate how many standard deviations an event deviates from the mean. They have many advantages, including low computational cost, no training required, and thresholds that are easy for teams to understand and operationalize during the early stages of FinOps. However, issues identified in (Boniol et al., 2024) include that Z-scores assume a stable distribution and can generate false positives on multimodal or non-stationary data; they also struggle to detect multivariate anomalies that require correlation analysis between metrics. Consequently, Z-scores are often suggested as a first-line alerting mechanism, which can be supplemented later with clustering, robust statistical methods, or ML approaches (Isolation Forest, autoencoders).

METHOD

This research was conducted using a descriptive quantitative approach using an anomaly detection model based on Z-Score statistical analysis. The Z-Score method was chosen because it provides accurate results in detecting anomalies, especially in datasets with limited data. This is relevant to a study (Nanekalva, 2025), which showed that Z-Score is a competitive statistical method for detecting anomalies in cloud metrics such as CPU and network usage. In comparison, in very large and dynamic cloud systems, machine learning or embedding-based approaches, such as those in (Mitropoulou et al., 2024), can better handle heterogeneity and high data volumes.

While many advanced approaches based on machine learning and deep learning exist, statistical methods remain relevant as the initial step in the FinOps pipeline. The use of Z-Score enables early warning processes with minimal computational requirements, allowing implementation without complex analytical infrastructure. Several studies also support the effectiveness of this simple approach; For example, a study (Olausson, 2024) demonstrated the successful use of Isolation Forest for real-time cloud metrics monitoring, while (Wang et al., 2021) introduced a self-evolving method that automatically adjusts detectors to reflect changes in cloud workloads. These findings suggest that more complex alternatives are available, but they often require high computational costs and model training processes that are not always necessary in the early stages of FinOps.

In this context, the Z-Score is a suitable choice because it is easily understood by cross-functional teams such as engineering, finance, and management, and can provide anomaly detection without model training. These factors make it an effective method for providing early warning of potential cloud cost spikes while generating structured risk analysis. In addition to highlighting cost deviations, the Z-Score also provides a quantitative basis that can be used to support decision-making, such as identifying high-risk months, understanding changing cost patterns, and determining which services need to be evaluated or reconfigured. Thus, this method directly contributes to the development of a more efficient cloud cost control strategy.

Overall, the analysis flow in this study consisted of the following steps:

Picture 1

Research analysis flow

The first stage is data collection, where data is taken from the Azure cost analysis dataset for the 2023–2024 period, which contains information on dates, service types, and total monthly costs. This dataset was chosen because it provides real-world spending patterns for Azure services such as virtual machines, storage, and DNS. Second, Data Cleaning and Preparation: Data is examined to remove blank values, duplicates, and adjust date and number formats. Next, monthly costs for each service are collected to facilitate the analysis of spending patterns. The next stage is the Basic Statistical Calculation stage with deviation analysis based on the calculation of standard deviation and average historical costs. To calculate the Z-Score, these values are used as the main parameters. Fourth, Using the Z-Score Method: The monthly cost value can be calculated using the following formula:

Alifah, D.S., Wardana, M.R., Cahyani, Y., & Albana, I. *Economic, Management, Business and Accountancy International Journal*, 2 (2) 2025, 74-78

ISSN 3110-6366 (online) DOI: doi.org/10.21009/EMBAIJ.002.2.5

$$Z = \frac{X - \bar{X}}{\sigma}$$

Picture 2
Z-Score Formula

In simple statistical outlier testing, a Z-score exceeding 1.7 is considered an anomaly. Therefore, in the Cost Risk classification, months exhibiting anomalies are categorized as follows:

Table 1.
Cost Risk Classification

Z-Score	Risk Category
Z < 1.0	Low Risk
1.0 ≤ Z < 1.7	Medium Risk
Z ≥ 1.7	High Risk

Based on the level of cost deviation, risk score = Likelihood × Effect.

The next stage is Perception and Interpretation: Monthly trend charts are created using Python, including pandas, numpy, and matplotlib, to show cost growth, peaks, and comparisons with historical averages. These visualizations help understand the context of anomalies and provide insight into factors that may be causing cost spikes. The final stage is Validation and Discussion: To ensure that anomalies align with changes in service activity, detection results are compared with Azure service usage patterns, such as VMs and storage. This validation demonstrates that the Z-Score is a simple yet accurate method for the initial FinOps process. For data processing, statistical calculations, and cloud cost trend visualization, this study uses the Python programming language with the pandas, numpy, matplotlib, and scikit-learn libraries. Python was chosen because it has a comprehensive and easy-to-use data analysis library and supports the replication of FinOps analysis processes.

RESULTS AND DISCUSSION

A Z-Score of 2.275 in April 2024 indicates that costs were more than 2 standard deviations above the historical average. Because it exceeded the threshold of ≥ 1.7, the month was categorized as High Risk. Statistically, this value indicates a significant anomaly that deviates from normal cost patterns.

This increase typically occurs due to increased usage of resources that contribute high costs, such as Virtual Machines and Storage. VMs with premium configurations, increasing the number of instances, or increasing storage volume can result in cost spikes consistent with the Z-Score pattern.

These detection results demonstrate that the Z-Score method is capable of quickly and efficiently identifying cost deviations without the need for complex models. This finding aligns with previous research on Cloud-based Anomaly Detection (CAD) and CNN-LSTM models, which both highlight the importance of detecting changes in usage patterns as an early indicator of anomalies. However, the Z-Score offers advantages in terms of simplicity and minimal computational requirements, making it effective for initial cloud cost analysis.

CONCLUSIONS AND SUGGESTION

Conclusion

This study successfully applied the Z-Score method to detect cloud cost anomalies in Microsoft Azure services. The analysis revealed one period categorized as High Risk, indicating a significant cost spike compared to the historical average. A Z-Score exceeding this threshold indicates a sufficiently extreme deviation, statistically categorizing it as an anomaly.

Alifah, D.S., Wardana, M.R., Cahyani, Y., & Albana, I. *Economic, Management, Business and Accountancy International Journal*, 2 (2) 2025, 74-78

ISSN 3110-6366 (online) DOI: doi.org/10.21009/EMBAIJ.002.2.5

The Z-Score implementation has proven effective because it allows for rapid identification of changes in cost patterns without requiring complex models or extensive computing resources. In a FinOps context, this approach supports cost oversight by providing early warnings of potential waste or uncontrolled resource consumption. Therefore, the Z-Score can be a practical early detection tool before organizations implement more sophisticated analytical methods, if necessary.

Suggestion

Future researchers are encouraged to explore other anomaly detection methods, such as Isolation Forest, ARIMA, or deep learning-based models like LSTM and CNN-LSTM, to compare their performance with the Z-Score method. This comparison is important to see how different approaches handle different data characteristics, such as seasonal patterns, time dependencies, or more complex service usage variables. Furthermore, varying methods allows researchers to assess other aspects such as detection stability, sensitivity to small data changes, and potential accuracy improvements in evolving cloud environments

REFERENCES

Aljanabi, M., Abd-alwahab, S. N., Rohmat, R. D., & Raad, H. (2021). *Cloud Computing Issues , Challenges , and Needs : A Survey*. *5*(September), 298–305.

Bhardwaj, P. (2021). *Optimizing FinOps Practices with Azure Cost Management and Billing Tools*. *9*(3), 1–8.

Boniol, P., Liu, Q., Huang, M., Palpanas, T., & Paparrizos, J. (2024). Dive into Time-Series Anomaly Detection: A Decade Review. *Proceedings of Make Sure to Enter the Correct Conference Title from Your Rights Confirmation Emai (Conference Acronym 'XX)*, *1*(1).

Islam, M. S., Rakha, M. S., Pourmajidi, W., & Sivaloganathan, J. (2020). *Anomaly Detection in Large-Scale Cloud Systems : An Industry Case and Dataset*. 1–12.

Katsarou, K. (2020). *A Systematic Review on Anomaly Detection for Cloud Computing Environments*. 83–96. https://doi.org/10.1145/3442536.3442550

Mitropoulou, K., Kokkinos, P., Soumplis, P., & Varvarigos, E. (2024). *Anomaly Detection in Cloud Computing using Knowledge Graph Embedding and Machine Learning Mechanisms*. https://doi.org/10.1007/s10723-023-09727-1

Nanekalva, B. (2025). *A Comparative Analysis of Statistical Anomaly Detection Methods for Cloud Service Monitoring : A Simulation-Based Evaluation Framework Methods for Cloud Service Monitoring : A Simulation-Based*. 0–7.

Olausson, K. (2024). *A Study on Isolation Forest for Anomaly Detection in Cloud-Based Systems*.

Sikha, V. K., & Siramgari, D. (2023). *Finops Practice Accelerating Innovation on Public*. *March*, 552–562.

Wang, H., Guo, J., Ma, X., Fu, S., Yang, Q., & Xu, Y. (2021). *Online Self-Evolving Anomaly Detection in Cloud Computing Environments*. 1–10.

Yakkanti, P. R. (2025). *AI-Enabled FinOps for Cloud Cost Optimization : Enhancing Financial Governance in Cloud Environments*. *13*(11), 17–29.

ISSN 3110-6366 (online) DOI: doi.org/10.21009/EMBAIJ.002.2.5