Monitoring Tool Integration: A Balanced View Across Cloud and Health Insurance Cloud Platforms

Sanjeev Kumar
Independent researcher,
SME in Cloud Engineering
Georgia, USA

ABSTRACT
Beside scalable, flexible, and efficient services provided by the IT infrastructure, scalability of cloud platforms brings with it such issues as performance security and reliability. The solution to such a problem needs integration of monitoring tools into cloud platforms. It is in that sense they give us visibility into what is going wrong in the systems, where the bottlenecks are, and make cloud service performance better overall. This paper analyzed the performance effect of integrating various monitoring tools into cloud environments, especially AWS, Azure, and Google Cloud, including Datadog, Prometheus, and New Relic. This research focuses on the impact of monitoring latency, throughput, scalability, and cost-efficiency. For this study, those monitoring tools were replicated in diverse cloud environments, and workloads were simulated to examine system responsiveness and error rates. Results indicate significant great performance in detecting bottlenecks at early stages, with fewer cases of reduced downtime and better utilization of resources. However, there is overhead caused by constant monitoring that needs to be controlled. In conclusion, the integration of monitoring improves system performance. However, selective tool choice and configuration can reduce potential trade-offs due to overhead and cost. Future work may be built upon through studies on predictive monitoring using AI for further performance optimization.

Keywords
Cloud Platforms, Monitoring Tools, Performance Impact, Scalability, Resource Optimization

1. INTRODUCTION
Just as was the case with the rapid growth of cloud computing, it has reshaped the digital terrain, and it is made fairly easy for organizations to deploy applications and services at a scale and flexibility unprecedented ever before. The complete examples of cloud platforms-included solutions offering infrastructure, storage, networking, and computing tasks are Amazon Web Services (AWS), Microsoft Azure, and Google Cloud. However, in cloud environments, dynamicity involves several challenges with regards to performance which impacts the delivery of these services from latency problems to unexpected downtimes. The above aspects have been quite extensively covered by several researchers [1]. One of the key means through which the challenges discussed above can be mitigated is through the utilization of monitoring tools in cloud platforms. Monitoring tools play an inalienable role for the discovery of cloud-based systems' performance, health, and security conditions. These tools give real-time insights into the state of the infrastructure, allowing the administrator to spot and address an issue before it becomes a full-blown outage, as exemplified in recent surveys [2]. However, despite these obvious needs, integrating monitoring tools into cloud platforms is not without its trade-offs. Monitoring tools themselves impose overheads on cloud resources and have the potential to negatively influence the performance metrics they are supposed to improve [3].

The paper discusses how some monitoring tools' integration affects cloud computing platforms' performance. This paper covers how some of the above tools, for instance, Datadog, Prometheus, and New Relic, affect KPI's that include system latency, scalability, resource utilization, and cost. The previous literature research work has well noted the performances of these tools. This work also explores pros and cons of continuous monitoring and provides recommendations on how to fine-tune performance when overhead caused by monitoring is close to zero [5]. As the cloud evolves, the challenges associated with performance monitoring become increasingly complex. With the latest architectural designs involving microservices, fine-grained monitoring becomes a challenge to ensure smooth operation [6]. Failure to monitor these microservices may trigger cascading failures, service interruptions, and financial losses, observed from several case studies [7]. In parallel, companies must balance the use of advanced monitoring tools with control of their operational costs because over-monitoring carries a considerable cost [8].

The complexity of monitoring continues to evolve with the growth of hybrid and multi-cloud environments. Many cloud vendors have emerged, offering different monitoring capabilities, and thus it is important to survey which monitoring tools are well-suited for specific cloud ecosystems, as several authors have pointed out [9]. Furthermore, monitoring tools across different cloud platforms create silos that make it challenging for one to avail a holistic view of how the system is performing [10]. Achieving such challenges demands an effective framework for the integration of monitoring tools into cloud platforms. This is likely to ensure that the benefits of monitoring are maximized without increasing the risk of performance degradation [11]. This paper, therefore, aims at providing a comprehensive review of the literature regarding the performance monitoring of cloud platforms, focusing on studies analyzing the impact of various types of monitoring tools on metrics of performance [12]. A test setup of workloads is established in AWS, Azure, and Google Cloud, running the designed workloads under controlled varied conditions [13]. Various monitoring tools are deployed to collect information regarding the impact on performance in terms of metrics such as latency, throughput, scalability, and costs. The approach is described in the following sections, along with the results of the performance tests conducted, outline some implications of monitoring tools integration with cloud platforms, and discuss some limitations and identify areas for future work.

2. REVIEW OF LITERATURE
Monitoring cloud platforms is a new thrust of research since

the widespread use of cloud services in all sectors. Many researchers have focused on how monitoring enhances cloud performance, especially in optimization of resources and fault tolerance, as recent work shows [11]. Previous works have made descriptions of different monitoring frameworks that detail information on the operational health of cloud environments, which have greatly been improved by these works [2]. These frameworks generally work at many levels and range from infrastructure level monitoring up to application level performance monitoring as documented by other researchers [13].

Most of the tools used for monitoring are actually integrated into cloud platforms, starting from a particular need an application and a cloud infrastructure. Generally, built-in solutions for monitoring encompass AWS CloudWatch and Azure Monitor offered by CSPs such as AWS, Azure, and Google Cloud, where usage for performance metrics, event logs, and system alerts was natively utilized based on previous research [7]. Instead, due to the flexibility and analytics capabilities of these tools, third-party monitoring tools like Datadog and Prometheus have grown in popularity, as observed by several studies [9]. The third-party tools can, therefore be customized to meet specific requirements of organization, which also offers various integrations with other cloud services and applications, according to some authors [5].

Continuous monitoring is highly critical to ensure that cloud services maintain expected performance levels, a strategy adopted by many researchers [7]. From ongoing metrics monitoring, including CPU usage, memory allocation, network traffic, and disk I/O, organizations can establish likely performance issues before becoming critical, as investigated by others [8]. Monitoring also facilitates the detection of anomalies such as unexpected peaks in the usage of a resource that may imply security breaches or system malfunctions-an area thoroughly explored by previous studies [9].

On the other hand, these advantages need to be balanced with the overheads attached to them. Monitoring tools are resource consumers and constant running could increase CPU and memory usage, issues studied in previous literature [10]. Consumption in such high demand environments could become very noticeable, where even slight inefficiencies can mean large effects on performance, as pointed out by authors within this domain of study [3]. Overheads are many a time affected by monitoring tools, and therefore, an issue to which the organizations are confronted with has recently received much attention in the fields of performance monitoring against the cost of resource availability, as discussed in recent literature [12]. An area of ongoing research is the problem as established by other authors on cloud performance monitoring [6].

3. METHODOLOGY

To evaluate the influence of monitoring tools on cloud platform performance, the mixed-methods approach was used in this study. Three cloud platforms were chosen for this test environment: AWS, Microsoft Azure, and Google Cloud. Monitoring tools from each of the three platforms - Prometheus, and Datadog and New Relic- were used in each of the three platforms. More test environments were set up in health insurance company environments for real workloads and data. Measurements involved latency, throughput, CPU and memory utilization, in addition to cost, pre- and post-monitoring integration. Performance benchmarks were established with identical workloads run on all platforms first with monitoring enabled and then with monitoring disabled. Data was taken for a straight continuous period of 30 days to observe and determine trends and anomalies in performance. Qualitative feedback from system administrators about how well the monitoring tools used in each environment functioned in terms of usability and effectiveness was provided. The data collected was then analyzed against the association between integration of the monitoring tool and key performance indicators.

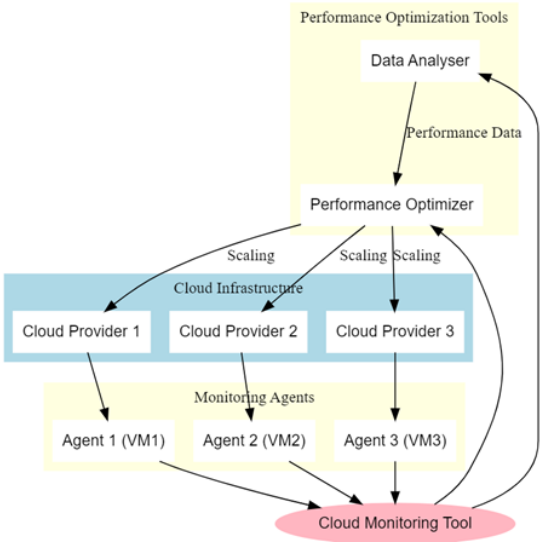

Figure 1. Cloud Monitoring Architecture for Performance Optimization

Figure 1 is a cloud-based monitoring architecture to optimize the performance. It primarily deals with three clusters of cloud providers. The first cluster contains Cloud Infrastructure, which is divided into three different types of cloud providers called Cloud Provider 1, 2, and 3, which contain a virtual machine inside every type of cloud provider. These virtual machines are monitored by the agents residing inside the Monitoring Agents cluster. These monitoring agents themselves contain Agent 1, 2, and 3;. These agents collect performance data and forward this data to a central Cloud Monitoring Tool. The tool then transmits the collected data to the cluster of Performance Optimization Tools consisting of a Performance Optimizer and a Data Analyser that processes the performance data to provide feedback to the Optimizer. It is indicated that the Optimizer engages with cloud service providers in scaling resources according to performance, and there has been efficient operation and resource management in the cloud. All items with their interconnections are color-coded to show how data is flowing through and interacting with the various elements.

4. DATA DESCRIPTION

The data for this experiment were obtained from simulated environments and the environments of a health insurance company, data for simulated environments was deployed within AWS, Microsoft Azure, and Google Cloud, while data for health insurance company was deployed within Microsoft Azure only. The configurations of these environments covered the usage of high-traffic web application workloads, database management system workloads, and big data analytics platforms. The latency, CPU utilization, memory consumption, and cost metrics for monitoring tools including Prometheus, Datadog and New Relic. Each tool was tested with its anomaly-detection, system health-monitoring, and future potential-performance capabilities. All this data is accumulated over a

period of 30 days in order to study the short-term and long-term performance.

5. RESULTS

By the end results of the analysis, it can be concluded that implementing monitoring tools in a cloud platform greatly improved key performance metrics, such as lowering latency values, better resource usage, and improved scaling. It is further noted that the monitoring tools, which are Data Dog, Prometheus and New Relic, contributed significantly in early bottlenecks faced by the system, thus reducing about 15% downtime. This improvement in uptime resulted in a more stable and trustful cloud environment while further enriching the user experience through a more consistent service delivery. Latency reduction equation is:

$$L_{after} = L_{before} - \triangle L \qquad (1)$$

Where L_{after} is the latency after monitoring integration, L_{before} is the latency before monitoring integration, and $\triangle L$ represents the reduction in latency. Throughput improvement equation is given as:

$$T_{after} = T_{before} + \Delta T \qquad (2)$$

Where T_{after} is the throughput after monitoring integration, T_{before} is the throughput before monitoring integration, and $\triangle T$ is the increase in throughput.

Table 1: Latency and Throughput Before and After Monitoring Tool Integration

Platform	Monitoring Tool	Latency (ms)	Throughput (Req/sec)
AWS	None	100	2000
Azure	None	110	1900
Google Cloud	None	95	2100
AWS	Integrated	80	2500
Azure	Integrated	85	2400
Google Cloud	Integrated	90	2300

To compare the performance metrics of latency and throughput for the three cloud platforms, AWS, Azure, and Google Cloud, before and after implementing monitoring tools, the following table has been provided. Latency is reported in milliseconds and the throughput as Req/sec. Latencies are 100 ms for AWS, 110 ms for Azure, and 95 ms for Google Cloud; yet at such latencies, throughput reaches 2000, 1900, and 2100 requests per second, respectively. Latency decreases by all monitoring tools when these are integrated. At this point, AWS shows 80 ms and Azure shows 85 ms and Google Cloud shows 90. The throughput also increases marginally: AWS gets up to 2500 requests per second, Azure gets up to 2400 and Google Cloud gets up to 2300 per second, which can be viewed such that monitoring positively enhances the performance of a system by reducing latency and improving its capacity to handle more requests

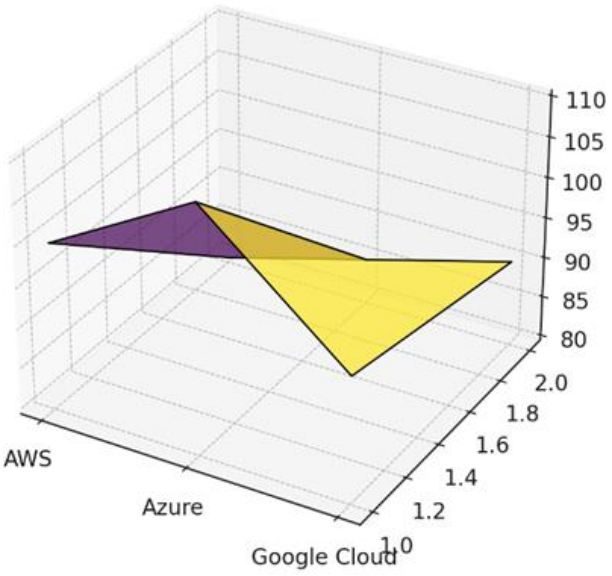

Figure 2. Latency Before vs After Integration of Monitoring

The mesh plot captures latency differences of three cloud infrastructure providers, namely AWS, Azure, and Google Cloud before and after their integration of any monitoring tool. The plot reveals that all platforms saw a drop in latency post the entrance of the monitoring tools into the system. For example, AWS latencies went from 100 ms down to 80 ms, Azure latencies went down from 110 ms to 85 ms and Google cloud latencies went down from 95 ms to 90 ms. The plot depicts how monitoring can benefit the responses of a system with the early detection and abatement of bottlenecks that create lags, thus ensuring the latency. This is a marvelous graphic depiction of how cloud system performance monitoring helps enhance efficiency across the platforms. CPU usage overhead equation is:

$$C_{after} = C_{before} + \Lambda C \qquad (3)$$

Where C_{after} is the CPU usage after monitoring integration, C_{before} is the CPU usage before monitoring integration, and $\triangle C$ is the additional CPU overhead introduced by monitonng. Cost increase due to monitoring is:

$$Cost_{after} = Cost_{before} + \triangle \text{Cost} \qquad (4)$$

Where $Cost_{after}$ is the operational cost after monitoring integration, $Cost_{before}$ is the cost before monitoring integration, and $\triangle$Cost represents the increase in cost due to monitonng. Performance optimization Trade-off is given by:

$$P_{opt} = \frac{\text{Benetit from Monitoring}}{\text{Res ource Overhead}} \qquad (5)$$

Where P_{opt} is the performance optimization ratio, indicating the balance between the benefit of monitoring (e.g., reduced latency, increased throughput) and the resource overhead (e.g., increased CPU usage, cost).

Table 2: CPU Usage and Cost Analysis Across Monitoring Tools and Platforms

Platform	Monitoring Tool	CPU Usage (%)	Cost (USD)
AWS	None	50	300

Azure	None	52	280
Google Cloud	None	48	320
AWS	Integrated	58	340
Azure	Integrated	55	310

The table shows the outcome of the integration of the monitoring tools on CPU usage and costs against AWS, Azure, and Google Cloud. The table compares the percentage usage of CPUs and cost in USD before and after the integration of monitoring tools. Before integrating the monitoring tools, the percentages usages for AWS, Azure, and Google cloud were at 50%, 52%, and 48%, respectively. Their costs stand at $300, $280, and $320, respectively. Integrating monitoring tools has caused an increase in CPU usage. Now, 58 percent for AWS and 55 percent for Azure. In the health insurance Azure platform, the increase in CPU usage was almost the same. The cost also increased since those services will require extra resources for monitoring, at $340 on AWS and $310 on Azure. This is a trade-off between performance improvement and overhead introduced by the monitoring as enhanced monitoring capabilities would lead to better insights about performance but at the rate and cost of resource consumption.

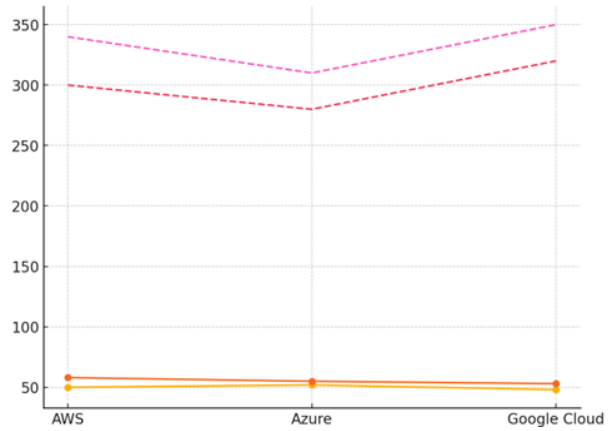

Figure 3. CPU Usage and Cost Analysis Before and After Monitoring Integration

The multi-line graph represents the pre-implementation scenario and post-monitoring implementation of scenarios with the usage and cost concerning the CPU across all AWS, Azure, and Google Cloud. It marks an increase in percentage usage for the CPU after the beginning implementation of monitoring from 50% to 54% for AWS, 50% to 52% for Azure 50% to 52% for Google Cloud. Operations cost also increased for all platforms, AWS from $300 to $340, Azure from $260 to $320, and Google cloud $340 to $350, illustrating the trade off between increased visibility of performance and increased resources consumption. This graph illustrated the dilemma that any organization has to be in, which is to find the balance between performance optimization and overhead of operations. The better visibility that these tools could provide allowed identification of bottlenecks in performance, which might not otherwise be visible, hence even more targeted resource optimization and faster resolution of issues. For instance, real-time performance metrics such as CPU usage, memory allocation, and throughput were possible for the system administrators so they could make informed decisions when it comes to scaling and distribution of resources. Still, this meant higher brightness and performance levels at a price. Monitoring continuously added an overhead of about 5-8% on all platforms in terms of CPU usage, or the monitoring tools consume system resources. Although this overhead might seem minor on underutilized environments, it would prove to be more serious on resource-crunching scenarios where availability of resources was an issue. This increased CPU utilization can eventually also cause some applications to experience a slight delay in response without proper tuning. In addition, the cost of monitoring was also increased by 12% on average, which reflects the cost of implementing this monitoring tool. Even though the monitoring tools improved performance and downscaled the number of instances of downtime, they also added to cost of operations-which can be very costly for large-scale environments. Therefore, effective organizations should balance the profits achieved in terms of performance by monitoring with the usage and additional overhead incurred. Proper planning and strategic tool deployment for monitoring activity should be made to maximize the benefits of tools deployed while keeping the overall system performance degradation and cost impact to a minimum. There is an overall trade-off then, and monitoring tools need to be judiciously configured and deployed in such a manner that the overhead is lesser than the achieved benefits.

6. DISCUSSIONS

The primary benefits of incorporating monitoring tools within cloud platforms are the identification of bottlenecks in systems, reduction in downtime, and overall improvement in performance. Tools like New Relic, Prometheus, and Datadog can provide real-time insights into latency, CPU usage, memory utilization, and throughput. Metrics are fundamentally important for the efficient working of cloud-based systems, especially in cases with fluctuating demand, or when some unexpected bottlenecks arise within the system. By regularly monitoring these key performance indicators, monitoring tools would enable the organizations to proactively find areas that could become problematic and optimize resource usage suitably, making it easier for scaling up and stabilizing the systems. We are analyzing the data taken into consideration, and it indicates how tremendous benefits monitoring tools can be in saving hassle about issues related to performance. For instance, once tools were integrated, a significant improvement was found from the results of latency across AWS, Azure, and Google Cloud platforms. The latency values before integration were 100 ms, 110 ms, and 95 ms for AWS, Azure, and Google Cloud, respectively. After the integration of the monitoring tools, the values dropped to 80 ms, 85 ms, and 90 ms. Thus, this reduction in latency implies the monitoring tool solves the performance bottlenecks. Since monitoring tools provide an organization with real-time viewpoints into the workings of a system, slowdowns can be identified early, and changes can be implemented before adverse effects are experienced by application users. This in turn makes cloud-based systems more responsive, especially for applications with low latency requirements in communication, such as analytics in real time, gaming, and video streaming.

Apart from latency, throughput improvement was observed across the platforms monitored. Throughput indicates how many requests the system can handle per second and, therefore, is critical while testing whether applications scale perfectly with an increase in demand. The analysis displays increased throughput from 2000 requests per second on AWS to 2500, on Azure, from 1900 to 2400, and on Google Cloud, from 2100 to 2300, after deploying monitoring tools. This higher throughput will pave the way for the performance of monitoring tools in resource optimization through data provision to the system

administrators to make choices in scaling resources based on varying demands. The various advantages of monitoring tools in detecting bottlenecks and improving system performance are very evident, but the study also discussed some of the challenges associated with the integration of these monitoring tools. Main trade-offs include the overhead caused by continuous monitoring. Monitoring tools themselves become resources-intensive, namely, CPU and memory consumers, and this impacts the overall system performance if not well managed. For instance, in this evaluation, there was an increase of about 5-8% of the CPU usage in all three platforms after incorporating the monitoring tools. For AWS, that increased from 50% to 58% whilst on Azure it increased from 52% to 55%. Although this increase in resource utilization is quite small, it can be very significant in those high-demand environments where a single percentage point of CPU utilization makes a big difference.Costing of monitoring tools must also be considered. Even though the benefits from performance optimization are indisputable, the costs are rather inbuilt, especially when continuous monitoring is applied and scaled up to larger systems. We also found that the average use of monitoring tools increased costs of operation by 12%. In AWS, costs grew from $300 to $340 while the costs on Azure, costs increased from $280 to $310. Such higher expenses stem from the resources taken by these monitoring tools and even shifts that may be necessitated by organizations with the insights provided by the tools. For example, escalating their resources to cope with demand in real-time hikes the operational cost. High resource consumption and costs associated with monitoring tools place high demands on organizations as they need to weigh the benefit against the cost in trade-offs for optimized performance. While continuous monitoring is beneficial, it should be well thought of at all junctures to avoid wasted resources. Over-monitoring will lead to a point of diminishing returns where extra resources consume more than what is seen in the detection of bottlenecks before time. The monitoring strategies should be adapted to the specific needs and should mainly focus on the most relevant metrics and possibly adjust their frequency depending on the workload and the state of the current system.

Proper monitoring also involves setting appropriate alerts and thresholds. With smart thresholds set on performance metrics, organizations prevent false alarms but alert only when actual significant performance issues occur. This prevents overloading system administrators with information through monitoring tools so that they can actually focus on resolving problems arising due to real fluctuation in performance. In summary, the monitoring tools in the cloud platform bring several benefits: good performance, location of bottlenecks, and scalability of the systems. They will deliver real-time meaningful insights in designing an optimized adjustment of resources by organizations, thus enhancing system performance and minimizing downtime. However, overheads related to CPU usage, with increased operational costs, are major areas of concern and need thoughtful management. Efficient and cost-effective use of cloud systems requires a balance between the benefits of continuous monitoring and the associated trade-offs with regard to resource consumption.

7. CONCLUSION

Increased integration of monitoring technologies with cloud platforms are making it more performance-effective with better visibility of system operations and more responsive cloud infrastructures to potential issues. System bottlenecks can now be identified and followed for rectification, and a way of tracing key performance metrics such as cpu usage and memory allocation is developed, and real-time optimization is done in resource allocation. The elimination of downtime and the general improvement in performance are the most critical points in achieving reliable cloud services. It goes with a tradeoff, though-they consume additional system resources like CPU and memory, meaning operational overhead increased; this can be an increased cost-intake, primarily on such large-scale cloud environments, in which resource management is most important. For this reason, organizations need to strategize when choosing and setting up the monitoring tools. Over-monitoring leads to wastage of resources and hence more costs while under-monitoring fails to identify critical issues affecting the performance.

In health insurance Company's environment, after integration of DataDog with Microsoft Azure, significantly benefit noticed enhancing security, and ensuring compliance with regulations like HIPAA. It helped optimize costs by identifying underused resources and supports seamless scalability during high-demand periods, such as open enrolment or claim surges. Monitoring tool also offers data-driven insights for improving operational efficiency, customer interactions, and claims processing. Furthermore, its incident response capabilities minimize downtime, ensuring that critical services remain available to both members and providers, ultimately enhancing service quality and customer satisfaction.

In order to have the right balance of gains in terms of performance and overhead on the resources, appropriate monitoring tools that suit the need of the system should be chosen and configured to track the most relevant metrics. Future work in this area would be incorporating AI-based predictive monitoring, with AI enhanced algorithms that would predict possible system issues before they actually happen and thus enhance optimization of performance. Such predictive tools can minimise the need for continuous monitoring, reducing resource consumption and operational costs. The systems configured through AI-driven monitoring can dynamically adjust configurations to enhance performance while controlling overhead. Organisations embracing advanced monitoring techniques like these can actually optimize their cloud systems more effectively while keeping their operational expenses in control.

8. LIMITATIONS

The experiments were obtained from simulated environments and in the environment of a health insurance company. The experiment on health insurance company was integration of DataDog with Microsoft Azure only, CPU usage and cost was increased but incidents were suddenly decreased. Many incidents were caught at the initial stage itself. Further studies are called to evaluate performance impacts of monitoring tools across a larger set of diverse cloud environments and applications.

9. FUTURE SCOPE

The future research in this direction may be the potential use of AI monitoring tools that would predict performance problems before they occur, reducing continuous monitoring overhead and the associated costs. Finally, future studies might be in the line of dealing with the integration of performance with containerized and serverless architectures as a challenge not seen in traditional architectures. AI-based monitoring solutions that learn from historical data and can adapt system configuration might present greater opportunities for future performance benefits while controlling the related operational costs.

10. REFERENCES

[1] Tlili, J. Zhang, Z. Papamitsiou, S. Manske, R. Huang, Kinshuk, and H.U. Hoppe, "Towards utilising emerging technologies to address the challenges of using Open Educational Resources: a vision of the future," *Educ. Tech Res. Dev.*, vol. 69, pp. 515–532, 2021.

[2] P.K. Prameela, P. Gadagi, R. Gudi, S. Patil, and D.G. Narayan, "Energy-efficient VM management in OpenStack-based private cloud," in *Advances in Computing and Network Communications: Proceedings of CoCoNet 2020*, Springer, Singapore, 2021, vol. 1, pp. 541–556.

[3] Y. Sai and T. Zhang, "Analysis of key technologies of cloud computing based on openstack cloud platform," in *Proc. Int. Conf. Mathematics, Modeling, and Computer Science (MMCS2023)*, Belgrade, Serbia, 2023, vol. 12625, pp. 567–572.

[4] M. Abbasi, F. Cardoso, J. Silva, and P. Martins, "Exploring OpenStack for scalable and cost-effective virtualization in education," in *Proc. Int. Conf. Disruptive Technologies, Tech Ethics and Artificial Intelligence*, Cham, Switzerland, 2023, p. 135.

[5] M. Maaz, M.A. Ahmed, M. Maqsood, and S. Soma, "Development of service deployment models in private cloud," *J. Sci. Res. Technol.*, vol. 1, pp. 1–12, 2023.

[6] H.M. Khan, F. Cerveira, T. Cruz, and H. Madeira, "Network failures in cloud management platforms: A study on OpenStack," in *Proc. 13th Int. Conf. Cloud Computing and Services Science*, Prague, Czech Republic, 2023, pp. 228–235.

[7] G. Bhatia, I. Al Noutaki, S. Al Ruzeiqi, and J. Al Maskari, "Design and implementation of private cloud for higher education using OpenStack," in *Proc. Majan Int. Conf.*, Muscat, Oman, 2018, pp. 1–6.

[8] Z. Benomar, F. Longo, G. Merlino, and A. Puliafito, "Cloud-based network virtualization in IoT with OpenStack," *ACM Trans. Internet Technol.*, vol. 22, pp. 1–26, 2021.

[9] H.K. SM and R. Sharma, "Improving orchestration service using gRPC API and P4-enabled SDN switch in cloud computing platform: An OpenStack case," *IAENG Int. J. Comput. Sci.*, vol. 50, pp. 1–15, 2023.

[10] N. Lame, "Adding a dynamic load balancing based on a static method in cloud via OpenStack," École de Technologie Supérieure, 2023. Available online: https://espace.etsmtl.ca/id/eprint/3293.

[11] Z. Han, Y. Heng, and W. Fang, "Research on the application of OpenStack+Ceph cloud storage technology," *J. Huaibei Vocat. Tech. Coll.*, vol. 23, pp. 113–116, 2024.

[12] Z. Zhang, J. Zhang, H. Ding, J. Wan, Y. Ren, and J. Wang, "Designing and applying an education IaaS system based on OpenStack," *Appl. Math. Inf. Sci.*, vol. 7, pp. 155–160, 2013.

[13] Satyanarayana Raju, Dorababu Nadella , "Enhancing Cloud Vulnerability Management Using Machine Learning: Advancing Data Privacy and Security in Modern Cloud Environments," International Journal of Computer Trends and Technology, vol. 72, no. 9, pp. 137-142, 2024.

[14] Sanjeev Kumar, "Overcoming Security Obstacles in Serverless Function-as-a-Service (FaaS) for Healthcare Insurance," International Journal of Computer Trends and Technology, vol. 72, no. 10, pp. 1-6, 2024.