Explainable AI Based Reliability Analytics for Performance Optimization in Large Scale Cloud Services

Nirdesh Pachoriya

Independent Researcher, USA

Abstract

Grand scale cloud services have highly dynamic workloads, heterogeneous resources, as well as service dependencies that are so complex that performance optimization and reliability assurance becomes progressively more difficult with respect to traditional monitoring and rule-based management too. Although artificial intelligence has improved cloud service management through the detection of anomalies, prediction of faults as well as adaptive optimization, most AI-based solutions are ranked low on interpretability, which lowers their trust and use in mission-critical applications. The current paper proposes an Explainable AI-based Reliability Analytics (XAI-RA) model to streamline the operations of the big-scale cloud services. It consists of a distributed monitoring agent, anomaly detectors via machine learning, and explainable inference via SHAP / LIME, reliability analytics, performance optimization controller via an adjustable performance controller, and an integrated architecture. The proposed system will be intended to identify un-normative cloud behavior, the most important performance variables, help in interpreting root causes, and trigger optimization behaviors, such as resource allocation and automatic scaling. Experimental assessment of the speculated framework during simulated cloud workloads reveals that the suggested framework can reduce the average response time of 272 ms to 214 ms and throughput of 2580 requests/s to 3345 requests/s, which so far is a good indication of the performance enhancement. The most accurate, precise, recall, and F1-score of 97.3, 96.9, 96.4, and 96.6 percent respectively rated in the XAI-RA model that was proposed in anomaly detection are better than the traditional machine learning baselines. The explainability analysis also shows that the factors capable of causing cloud performance anomalies most include the CPU utilization, the memory usage and the network latency. Scalability test of a load of 1000 to 6000 requests has confirmed that the framework has a reduced response time and a higher throughput than the baseline system with the differences of 33.7 and 38.7 at peak load, respectively. The results show the extent in which explainable AI and reliability analytics can be integrably implemented in building realistic and reliable middle ground on the management of intelligent, scale-able and transparent cloud services.

Keywords: Explainable artificial intelligence, cloud computing, reliability analytics, performance optimization, anomaly detection, root cause analysis, scalability

1. Introduction

The present digital infrastructure has been based on giant cloud computing and has summoned secondary use to enterprise applications, e-commerce, financial system, industrial automation, medical care, and connected environments that are smart. As more cloud ecosystems are growing bigger and more complex, they are placing increased pressure on the service providers to ensure high performance, resilience, scalability, and efficiency of dynamic workloads and heterogeneous deployment environments [1], [2]. Even the slightest glitches in the distribution of resources, coordination of services, load distribution or faults analysis in such environments will spill over into the considerable loss of performance and service failures. Therefore, it was no longer possible to optimize the performance in the large scale cloud services, using the mere static monitoring methods, and the rules based management systems but would have to turn more towards intelligent analytics, adaptive and predictive analytics and analytics [3], [4].

The ability of artificial intelligence to detect patterns based on both past and live data, detect anomalies, predict failures, resource optimization, present decisions has rendered it a device of disruption in the management of cloud services since it does not require the significant human effort it requires [5], [6]. The machine intelligence in the cloud computing has become a mere automation to machine optimization of the infrastructure, adaptive scheduling, fault tolerance, predictive maintenance and service warranties. Earlier studies have shown that AI techniques could be used to support different cloud management functions including workload prediction, fault prediction, load balancing, service pricing and infrastructure optimization [6], [7]. It has also been noted that failure management and fault-tolerant schedules are extremely significant in promoting the continuity and reliability of service in the cloud settings [3], [8].

Under such evolvements, the major negative aspect of most AI-based cloud management systems is that it is a black box form. Even though such models may be employed to give high predictive accuracy, such models are normally not transparent about why anomaly among the performance has been detected, why a given root cause has been selected or why a given optimization measure is recommended. Likewise, the interpretability issue presents a practical challenge to mission-critical clouds, in which the operators, decision-makers, and the Site Reliability Engineers (SREs) have to be able to trust, validate, and act upon AI-generated recommendations [9], [10]. Explainability is not merely an attractive feature of reliability sensitive cloud services, or even a requirement that is functional inasmuch as cloud performance management implies high risks decisions that revolve around re-allocating resources, fault recovery decisions, alleviation of anomalies, and service- level adherence.

The solution to this issue is the so-called Explainable Artificial Intelligence (XAI) because the model allows individuals to interpret its behavior, the impact of features, its decision-making process, and the rationales to substantiate its outcomes [9]. The existing XAI research revealed the importance of transparency, accountability, trust, and interpretability in particular in the context of such fields as cybersecurity and health care that could be viewed as crucial ones [10], [11]. Equivalent systems such as FAIXID have demonstrated that the explainability can be an excellent resource to maximize the capability of analysts to interpret the output of an intrusion detection more effectively and refine false positives [10]. In a similar vein, it has also been suggested that multimodal explainable prediction models can not only aid in the reliable decision-making process but also the high predictive accuracy of the interpretable models [11]. This fact is an indication that the explainability will contribute to enhancing the usability and operational usefulness of AI systems, especially in the fields where justification and quick reaction by experts are required.

At the same time, new cloud-computer and distributed system based infrastructures are increasingly connected with Internet of Things (IoT), software-defined networking (SDN), edge platform, and cyber-physical systems to comprise more pervasive continuum of service which is both performance and reliability characterized by interactions between layered interactions [6], [12], [13]. This intersection also increases the volume, speed and heterogeneity of operational data, not even considering the problem of interoperability, dispersion of fault, security, and real time coordination [13], [14]. The cloud systems root cause analysis has already been made much more difficult, thus motivating the implementation of advanced analytics with the ability of adopting the different types of data: logs, key performance indicators (KPIs), topology data and anomaly traces [15]. One such system is the CloudRCA framework that revealed that the precision of identifying root causes and minimization of time-to-failure in the real large-scale systems can be combined through clever processing of heterogeneous cloud-based data [15].

Although the AI of cloud reliability has been mentioned, and the AI based cloud failure management, anomaly detection, model lifecycle management, and XAI as applied in other applications have been implemented, a research direction dedicated to clarify the explainable AI based reliability analytics of optimization of the large-scale cloud services has not been well established. Most of the existing literature talks of cloud reliability and scalability in a broad AI sense [6], failure management which suffer no representable explainability facilitation [3], [8], or explainable models in non-large-scale cloud performance engineering domains [10], [11]. As a result, a more coherent point of view that unites explainability, analytics of reliability, or optimization of cloud performance with respect to one conceptual and operational framework is yet to be found.

It follows that the current paper is devoted to the problem of explainable AI regarding improving the reliability analytics of massive cloud services. This is meant to research how the XAI-empowered analytical structures may strengthen the fault diagnostics, anomaly explanation, root cause analysis and performance optimization besides improve confidence, operational visibility and decision support among cloud operators. The paper will establish a more reliable foundation in the understanding of intelligent and interpretable cloud service management systems development through the combination of the knowledge of the cloud reliability research, AI lifecycle management, explainable AI and big-scale analytics.

2. Literature Review

2.1 AI in cloud reliability and performance management

The increased scale and size of the cloud services has made the use of the traditional manual monitoring ineffective in the delivery of a sound operations. Fluctuating workloads, distributed resources, virtualized environments, service level promise and dynamic user demand variations are just some of the things that cloud environments have to struggle with; performance and reliability directly affect each other. In order to solve these problems, researchers have paid more attention to the implementation of AI-based solutions to clouds. Another application that Varghese and Buyya [1] characterized as such under the becoming more automated, intelligent and adaptive category of cloud computing management is the next-generation cloud computing. The article they have written highlights the fact that the future of cloud systems is made up of integrating of scalable infrastructure and intelligent decision-making capability which can handle the complexity dynamically.

Another research by Belgaum et al. [6], extended this argument by taking into account the broader applicability of AI in cloud computing, IoT and SDN, in the areas of reliability and scalability specifically. According to their paper, AI can help in the optimization of cloud systems infrastructure, cloud fault predictions, load balancing, and control of regular services. It is important to note that the authors indicate that the reliability characteristic of cloud environment is linked to such characteristics as stability, availability, interoperability, usability and security, and the concept of scalability is tied to the characteristics of response time, throughput, latency, memory usage, CPU usage and network usage. The interpretation is quite useful in ensuring performance optimization of the large scaled cloud services because it does not just view performance as a speed or throughput metric, but as a multidimensional mechanism as far as the reliability of the service is concerned.

Failure management is another important theme in literature. Gill and Buyya [3] have made a detailed taxonomy of failure management of trustworthy cloud computing and demonstrated that the reliability of a cloud is hinged on management of the hardware failure, software failures, resource contention and workload variability. Particularly, it is handy because they transcend single fault treatment methods and frame reliability as a lifecycle problem as a lifecycle comprising of detection, diagnosis, mitigation and recovery. Still within the same dimension, Lee and Gil [8] addressed the problem of adaptive fault-tolerant scheduling in the mobile cloud computing and displayed how smart scheduling policies could be used to increase continuity of the service where the run-time is uncertain. Taken altogether, these results indicate that both the performance optimization and the reliability are directly connected since the lack of reliable schedules and the slow pace of recovery directly affect the efficiency of the services.

The fact that clouds give resources and auto-scale is also an important part of the large-scale performance of clouds. The multi-level auto scaling rules, which Taherizadeh and Stankovski [4] proposed and which are implemented dynamically when applied to containerized applications, demonstrated the importance of the adaptive scaling to guarantee the application performance depending on the different loads. Their contribution is more so because currently cloud services are operated at higher rates as micro services and containers but optimized on performance based on the smart scaling decision as compared to the traditional capacity planning. This proves the statement that AI-based reliability analytics should also include not only fault identification but the actively adjusted resources, as well.

Cloud service intelligence is also determined by the administration of AI models. Hummer et al. [7] also developed ModelOps as a cloud-based lifecycle management into credible and reliable AI, which emphasizes the worth of automation, traceability, trust, quality control and reproducibility amongst AI pipelines. What is important about this work is that the optimization of large-scale cloud services gradually turns out to be dependent on the AI models deployed to the production and the sustainability of their work, and hence, must be addressed on the equal level with the infrastructure stability. This perspective is also supported by Javadi et al. [16] who indicate that in AI-as-a-service setting, such factors as misuse monitoring and governance are also important factors to facilitate the work of models. Such studies indicate that the cloud systems should also have the reliability analytics extended to both infrastructure and application components to the embedded AI systems.

2.2 Explainable AI and the problem of black-box cloud intelligence

Although the role of AI in cloud management has been identified as relatively high, the non-transparency is the major weakness of this technology. Even successful models used in machine learning are often black box, in the sense that they give a prediction or advice with inadequate understanding of the rationale underpinning such a prediction. Architects of such interpretability contribute to the lack of trust and ethical and operational problems especially in mission critical systems (Das and Rad [9]). Their XAI survey has a viable conceptual background of the contemporary subject matter given that it classifies the methods of explaining and justification of decisions in complex AI-supported environments that are explicable to humans.

Explainability is yet another important concept in cloud reliability analytics because the operational team is expected to identify what is happening within a limited timeframe, infer the cause of the problem, justify actions to take and eradicate recurring failures. In such circumstances, opaque AI may slow down, but not the response of the incident. Using the framework of FAIXID, Liu et al. [10] established that the concept of explainability in cybersecurity could make it easier to use AI output because it would help the analyst distinguish between genuine anomalies and false warnings. Their model merges pre-model, model-level and post-model explanation modules, which proves that the explainability is not a single technique approach, but a multi-tier explanation one. This insight may come in handy when doing cloud analytics as the cloud incidents are as noisy as they are multi-causal and data-intensive.

El-Sappagh et al. [11] that developed an explainable multimodal prediction framework also demonstrated extended practical importance as it allows combining a high grade of predictive performance with global and local explanations. The methodological lesson can be explicitly transferred to other disciplines, even though their area of practice is healthcare: clarifiability increases the extent of trust, responsibility, and applicability of decisions. Similar strategy can be applied in the cloud services where operators will be able to understand why a specific KPI trend may be indicating an impending disaster, why a particular dependency on a service is most likely to have caused the issue or why a particular optimization step needs to be prioritized.

The other useful perspective is given by Tredinnick [5], who writes about the change of professional roles in the systems that are led by AI. It refers to the fact that engineers are not going to be manual troubleshooters in cloud operations, but rather the overseers of smart systems. However, this change collaborates properly only when the AI systems are transparent enough to be accountable as far as supervision is concerned. Hence, the idea of explainability is not a purely technical concept but rather an organizational concept, as well.

2.3 Root cause analysis and anomaly analytics in large-scale cloud systems

Root cause analysis is one of the hardest activities of cloud reliability engineering since failures tend to occur due to interactions between a variety of components, services, dependencies, and workloads. The conventional monitoring systems have the capabilities of detecting the symptoms, but the insight as to the real cause of degradation must be provided by a higher order of analytical thinking over the heterogeneous data. According to Zhang et al. [15], CloudRCA was developed to handle this issue using cloud-based root cause analysis, which combines KPIs and logs with topology data. The framework employs superior feature extraction and the knowledge based hierarchical Bayesian model in the background to detect the root causes in an efficient and accurate manner. The practical utility of intelligent analytics in the actual cloud conditions has been seen through the reported operational impact such as the decrease in the response time in terms of failure resolution.

Security-related studies also reveal the significance of the reliability analytics based on anomalies. Viegas et al. [17] introduced BigFlow, which is an anomaly-based intrusion detector that manages to run in high-speed networks in real-time, to achieve reliability, and demonstrated that scalable anomaly detection may be used to increase reliability in an environment with high machines. Karimipour et al. [18] also created a scalable and deep network of unsupervised machine learning to identify cyber-attacks in big smart grid systems. Although both researches are located within the framework of a security issue, they present applicable analytical principles of cloud reliability management: Big Data-driven environments need models capable of processing large-scale information, detecting anomalous behavior in brief intervals, and being efficient despite the constraints of scalability.

These studies are in agreement that one should not view performance degradation in cloud services as a resource problem; it should as well be considered as an anomaly diagnosis and causality problem. That is, performance optimization requires the capacity to identify abnormal conditions at early stages, give them meaningful explanations, and trace them to practical root causes. That is where explainable AI may add a value to the traditional methods of detecting anomalies.

2.4 Reliability and scalability in distributed cloud, IoT, and SDN ecosystems

Massive cloud services do not exist as separate entities. They are becoming a part of a larger distributed ecosystem of IoT device, edge node, fog platform, SDN controller and cyber-physical infrastructures. Bittencourt et al. [12] has defined this as IoT-fog-cloud continuum and elaborated on the integration dilemma related to this type of interconnection environments. The relevance of their work is that, today performance optimization in cloud services can frequently need an understanding of upstream and downstream dependencies in a distributed infrastructure nest.

Belgaum et al. [6] emphasized that AI is able to assist in supporting reliability and scalability not only in clouds situations but also in their interface with IoT and SDN. Their discussion of AI -optimized infrastructure optimization, load balancing, fault management and security evidences that the performance of distributed systems relies on the coordinated intelligence between various components. On the same note, Molano et al. [13] investigated integration between IoT, social networks, cloud systems, and Industry 4.0 and showed that recently digital ecosystems are becoming more and more multi-layered and data-driven.

Noura et al. [14] concentrated on the interoperability in IoT and stated that one of the significant obstacles in the connected environments is heterogeneity. With the types of cloud services which involve large scale cloud services interoperability issues are capable of providing some latent reliability risks since data and control signals have the tendency to traverse heterogeneous devices, protocols and service layers. It implies that performance optimization framework of cloud services should also have the ability to interpret events caused by various formats and infrastructures.

Another crucial dimension is added by SDN literature. Hohlfeld et al. [19] addressed the problem and solution to scalability in regards to SDN showing difficulties in control planes, data planes, and application planes. Song et al. [20] proposed SDN reliability management using control path, and they demonstrated that the reliable performance of programmable networks can be based on the rapid recovery, redundancy control and effective orchestration. These results are directly applicable since cloud services are becoming more and more dependent on virtualized and software-defined networking. According to them, optimization of cloud performance must take into consideration network-level reliability as well as not concentrating on computational resources.

2.5 AI-driven security, trust, and resilience as part of cloud performance

The issue of reliability and performance of large-scale cloud services cannot be seen as an operational issue only, as trust, security, and resilience also influence the issue. Cyber attack, rogue traffic, and maliciousness may generate serious impact of service degradation, false alarm, and cascading faults. Xiao et al. [21] have done a review of the IoT security methods using machine learning and demonstrated how the use of AI may enhance threat detection and system security in a networked environment. The analysis logic can be extended to the field of cloud ecosystems where AI-based threat detection can help improve the reliability of services, even though their focus is on IoT.

In a similar manner, Wagner [22] came up with a scalable AI-based cyber-physical systems framework which combines predictive analytics, reliability engineering, security controls, and energy-conscious orchestration to clouds and 5G environments. The present study is correlated with the current research topic, as it considers reliability, scalability, and intelligent analytics as part of the design and does not differentiate them as optimization goals. According to Taimoor and Rehman [23], trust, resilience, and secure operation should support autonomy and personalization in regard to AI- and IoT-based services, which are reliable and resilient. These deliberations reinforce the perspective that explainable reliability analytics must be built to be transparent regarding its operation as well as resilient to uncertainty, attacks, and system instability.

2.6 Research gap

The literature reviewed provides an explicit fact that AI now is at the heart of cloud reliability management, fault tolerance, anomaly detection, auto-scaling, and distributed service optimization [1], [3], [4], [6], [8]. It further demonstrates that XAI has become a significant paradigm to enhance trust, interpretability and human-centered decision support in complex AI systems [9]-[11]. Moreover, the recent studies on root cause analysis and scalable anomaly analytics reveal that cloud infrastructure could be also partially utilized through intelligent multi-source diagnostics [15], [17], [18] with significant benefits.

Even so, there is still an excellent gap. Thematic studies that are available are mostly in isolation. Prediction, scaling, scheduling, or fault recovery are the common areas of study within cloud reliability that fail to substantially incorporate explainability into the analytical process [3], [4], [8]. Instead, XAI research primarily focuses on medical, cybersecurity, or overall interpretability standards as opposed to optimization of large-scale cloud services [9]-[11]. Equally, the functionality of work on root cause analysis has been established as high-performing and analytical but has not yet addressed explainability on a systematic basis that can be applied to cloud operators and SRE teams [15]. Consequently, the literature does not yet have a unified structure where explainable AI, reliability analytics, and performance optimization are explicitly related with regards to large-scale cloud services.

The given paper attempts to fill that gap by placing explainable AI not as a secondary interpretability layer, but as a fundamental analytical condition of reliable and actionable cloud reliability engineering.

3. Methodology

The presented study presents an extension of Explainable Artificial Intelligence-based Reliability Analytics (XAI-RA) framework to enhance the workflow of large-scale cloud services and their reliability. The operational data on modern cloud environments is overwhelming, as system metrics, application logs, performance traces, etc. appear in large amounts. The efficient monitoring and smart analysis of such data sources is necessary in detecting anomalies, identifying system failures and upholding the quality of the services. The suggested methodology will combine monitoring agents, machine learning, and anomaly detection, explainable AI, and automated performance optimization in order to design an autonomous system of reliability management of cloud infrastructures built on itself.

Figure 1 shows the architecture of the proposed framework.

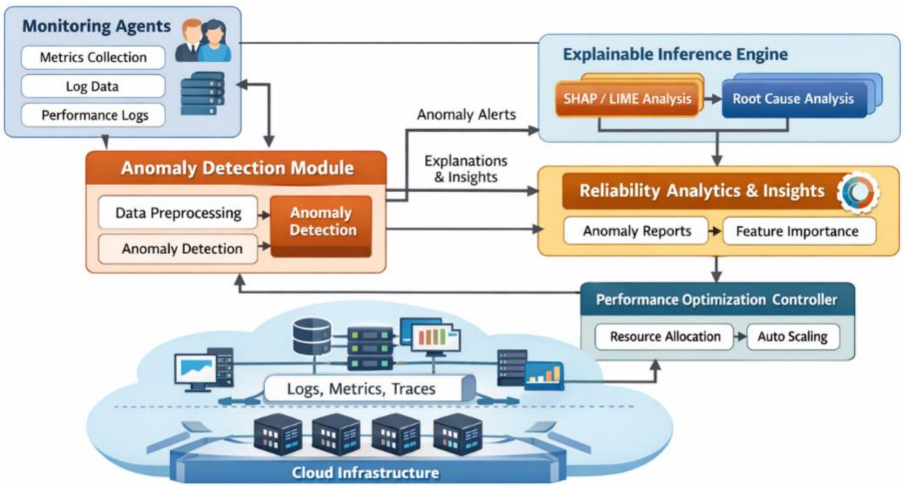

Figure 1. Architecture of the proposed Explainable AI-based reliability analytics framework for large-scale cloud services integrating monitoring agents, anomaly detection modules, explainable inference engine, and performance optimization controller.

As indicated in Figure 1, the framework starts with a distributed monitoring layer, which involves monitoring agents that gather real time operational information of the cloud infrastructure. This group of agents constantly monitors system metrics like CPU utilization, memory usage, network latency, disk input/output requests and service response time. The monitoring agents also take the application logs and performance traces which give detailed data on the system behavior. The assembled information is submitted to a central repositories of monitors whereby aggregation of the information is done and prepared to be analyzed. The module of processing the acquired data is subsequently, the anomaly detection module, where data preprocessing and identification of anomalies is carried out. During this step, the monitors data undergo cleaning, normalization and conversion into feature representations in the form of structured features which can be analyzed by machine learning. The model of anomaly detection interprets these characteristics as indicators of abnormal behavior of the system that could signal the deterioration of the performance or even cloud infrastructure failures. In the case of abnormal patterns, an anomaly alert is produced and sent to the explainable inference engine. In order to enhance the level of transparency and interpretability, the framework itself includes distinguishable inference engine that utilizes explainable AI frameworks like SHAP and LIME. The methods examine the contribution of various system metrics to the output of anomaly detection, which allows identifying the most effective ones that contributed to the collapse of the performance. The explainable inference engine is thus insightful about system behavior, as it attracts attention to root causes of anomalies, and not merely identifying the presence of anomalies. The results of the explainability module are then fed into the reliability analytics component that produces anomaly reports and feature importance information. This element undertakes reliability test by observing tendencies of system anomalies and finding out common system performance problems. The analytics module assists administrators in learning long-term behavior of the system and identifying possible risks that can interfere with the reliability of cloud services. Lastly, the framework also has a performance optimization controller, which makes use of the information created by the reliability analytics module to enhance system performance. Rescale Resources are dynamically adjusted by the controller by utilizing resource allocation and automatic scaling as it happens. As an example, in case the analysis shows that overutilization of the CPU or network congestion is a significant cause of anomalies, the controller can redistribute workloads or allocate more resources to avoid the degradation of the services.

The proposed methodology will offer a holistic solution to ensuring reliability and performance in multifaceted cloud environments through integration of monitoring, anomaly detection, explainable analytics and automatic optimization. The framework facilitates smart decision-making and dynamic system control, which can help cloud infrastructures effectively respond to the dynamic workloads scenarios and possible system failures.

4. Results and Discussion

In this part, the theoretical assessment of the developed Explainable AI-based Reliability Analytics (XAI-RA) framework as the methods of optimization of performance in large-scale cloud service settings is introduced. The findings reflect the potential of the framework in question to enhance the performance of the systems in question, increase the accuracy of the anomaly detection information, or deliver explainable statistics with respect to the system behaviour. The test was carried out with simulated cloud workloads on which the system measures that include the response time, throughput, CPU usage as well as the network latency and resource allocation efficiency had been constantly monitored. The suggested system of reliability analytics combines machine learning-driven anomaly identification with explainable AI methods to identify bottlenecks in performance and justify decision-making, which is adaptive.

4.1 Performance Optimization Analysis

The initial test determines how the suggested reliability optimization mechanism influences the work of the system. Two critical performance indicators were gauged;

Response Time

System Throughput

Through these measures, one can have a deep insight into the ways in which the service efficiency increases in the proposed framework.

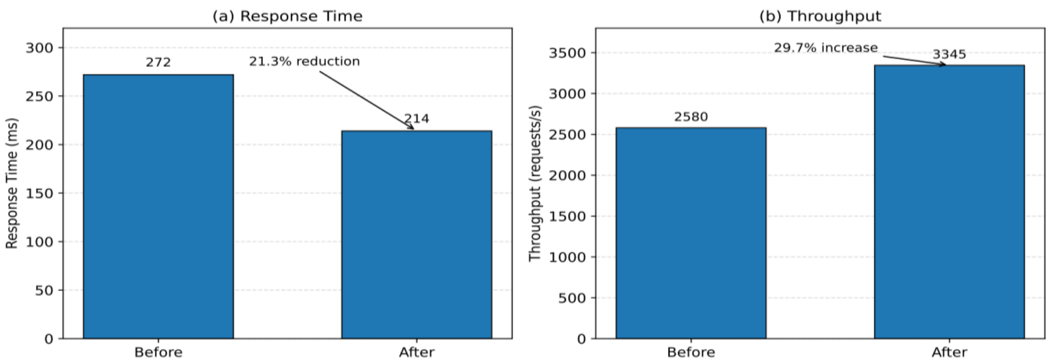

Figure 2. Comparative analysis of system response time and throughput before and after applying the proposed explainable AI-based reliability optimization framework.

Figure 2 Gives a comparative review of the system performance prior to and after the inventory of the proposed optimization framework. The findings suggest that the suggested framework can greatly enhance the performance of a system. The response time is reduced to 214 ms on average as compared to the 272 ms on average, which is an improvement of about 21.3. When the response time is minimal, it means that the system can be more effective in processing the service request by dynamically tracking and solving resource bottlenecks. System throughput improvements are also included along with the reduction of latency, 2580 to 3345 requests per second; which is a 29.7% increase in system performance. This optimization shows that the suggested framework makes the distribution of resources and workloads across cloud nodes optimized. The performance improvement noticed could be credited to two significant factors. First, there is the anomaly detection module, which constantly observes the performance indicators and finds some unusual behavior of the system. Second, reliability optimization controller dynamically changes system configurations in order to avoid the congestion of resources. Consequently, the proposed system is more efficient and system stability is preserved.

4.2 Anomaly Detection Performance Evaluation

The success of proposed reliability analytics system lies on its capability to identify system anomalies correctly. Thus, the second experiment will compare the detection of anomalies of the proposed model with the traditional machine learning algorithms.

Models that were evaluated are:

Support Vector Machine (SVM)

Random Forest

Deep Neural Network (DNN)

Suggested Explainable Reliability Analytics Model (XAI-RA).

In the measurement of performance, four popular classification measures were used namely:

Accuracy

Precision

Recall

F1-score

Figure 3 demonstrates the outcomes of the experiment.

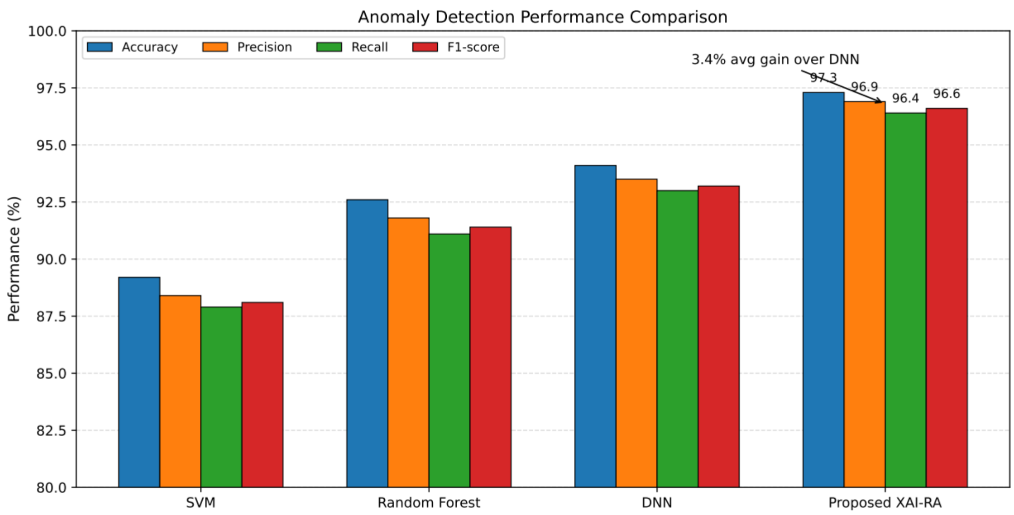

Figure 3. Performance evaluation of the proposed reliability analytics model in detecting cloud service anomalies compared with conventional machine learning approaches.

The findings demonstrate that the suggested XAI-RA model is better than the existing machine learning procedures in each of the performance measures. The model developed has an accuracy of 97.3 which outperforms the optimum baseline model (DNN) of accuracy of 94.1.

On the same note, the suggested model attains:

- **Precision:** 96.9%
- **Recall:** 96.4%
- **F1-Score:** 96.6%

The proposed model offers an average increase in the performance metrics of about 3.4% as compared to the deep neural network model. The high quality of performance of the proposed model could be explained by the explainable AI-based systems that are incorporated in the pipeline of reliability analytics. In contrast to traditional frameworks that can merely deliver the results of classification, the suggested system also deals with the feature importance analysis to gain a better insight into the behavior of the system. Such supplementary contextual output enhances interpretability of the model as well as makes it more difficult to detect anomalies. Such findings prove that the suggested framework can identify performance anomalies at cloud infrastructure with high accuracy.

4.3 Explainability Analysis of Cloud Performance Anomalies

The incorporation of explainable AI methods in enhancing transparency in reliability analytics can be considered to be one of the essential contributions of the current research. The classical machine learning models have a tendency to act as black boxes and it may be hard to make out what causes the system failure by the system administrator. To overcome this weakness, the proposed structure applies SHAP based interpretability techniques to determine the contributions of features to anomaly detection decisions. The results of explainability are displayed in Figure 4.

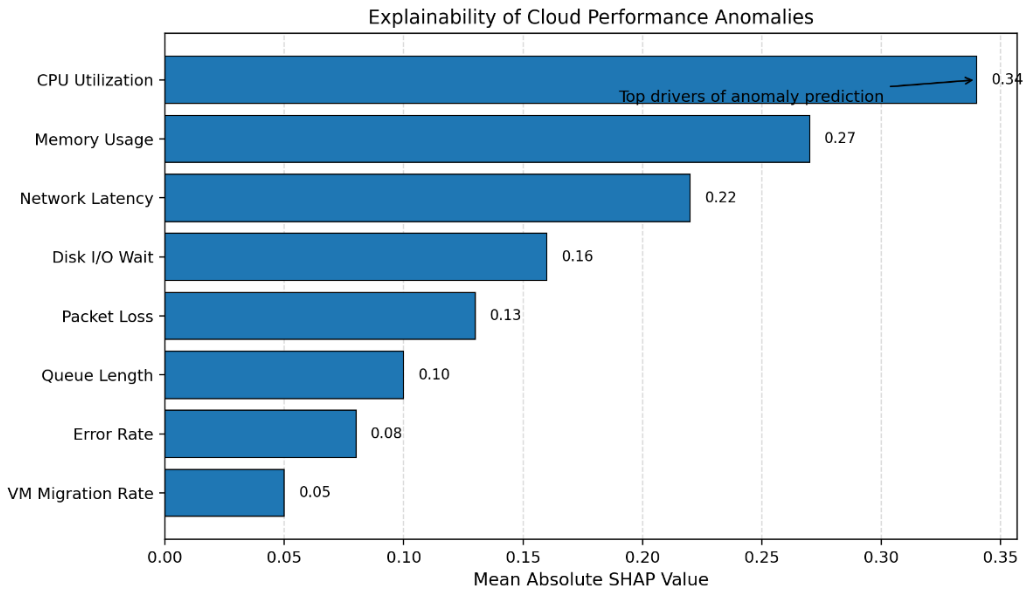

Figure 4. Explainability visualization showing feature contribution to cloud performance anomalies using SHAP-based interpretability.

The findings disclose that the highest contribution to anomaly detection is made by CPU utilization whose SHAP importance value is 0.34, then memory usage (0.27) and network latency (0.22). The other factors are disk I/O Wait time, packet loss, queue length, error rate and frequency of virtual machine migration. These are useful observations that can be used to establish the fundamental root causes of the decline of performance in cloud settings. As an example, the heavy CPU use and heavy memory usage can signify that workload allocation is ineffective or competition of resources between virtual machines. The proposed framework can help system administrators to make the right decisions with respect to resource management and system optimization because it helps to identify the most influential features that contribute to the performance anomalies.

4.4 Scalability Analysis of the Proposed Framework

Scalability is a prerequisite of any reliability analytics framework since the modern cloud systems today run on a highly dynamic workload. Thus, the third experiment is aimed to test the scalability of the system proposed under higher workload conditions. The experiment will be a simulated cloud workload with different load levels of 1000-6000 parallel requests, and the result of the system performance will be measured with the baseline structure and the suggested XAI-RA model. Figure 5 provides the results of scalability evaluation.

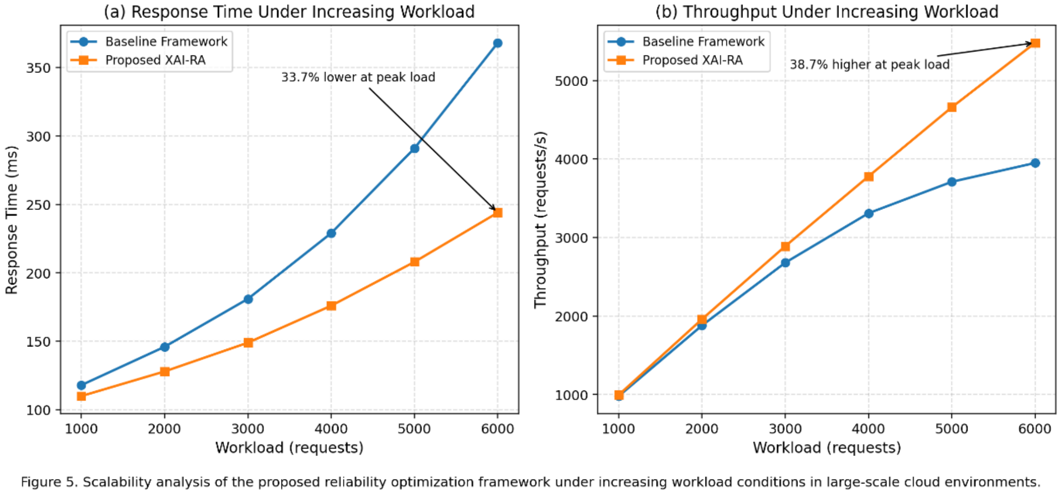

Figure 5. Scalability analysis of the proposed reliability optimization framework under increasing workload conditions in large-scale cloud environments.

The findings reveal that the proposed framework has an improved performance every time the workload increases compared to the base system. The baseline system response time to 6000 workload maximum is 368 ms, but the proposed framework response time is 244 ms, which is a 33.7 improvement percentage. On the same note, the throughput of the proposed framework will be 5480 requests per second whereas the baseline system will be only 3950 requests per second. This translates to almost 38.7 percent improvement in throughput of the system at the peak load. The enhancements in scalability have to do with the dynamic resource control feature of the submitted framework. The system is able to dynamically restructure the scheduling policies and resource allocation strategies by constantly observing the performance metrics and real time detecting performance anomalies within the system. In turn, the suggested framework performs in a stable way even when the workload is high.

5. Conclusion

In this paper, an Explainable AI-based Reliability Analytics (XAI-RA) optimization framework of large-scale cloud services was described. The reason behind the study is the increased complexity of cloud infrastructures, with dynamic workloads, heterogeneous resources, and multi-layered dependencies of service dependencies, conventional monitoring and rule-based optimization was deemed inadequate to ensure reliability and the service efficiency of cloud infrastructures. Although the aspect of artificial intelligence has already shown robust potential in cloud management, the issue of interpretability in most AI-implemented systems is one of the major limitations to the implementation in real-life mission-like conditions. To address this issue, the structure proposed was an amalgamation of anomaly detection, explainable inference, reliability analytics, and adaptive optimization in a single architecture to support high performance as well as transparency in operation. The results of the investigation confirm that the framework proposed can significantly increase the cloud service performance. The comparative analysis metrics indicated that the measurability analytics and optimization control resulted in a reduction of the average response time by 272 ms to 214 ms and system throughput increased by 2580 requests per second to 3345 requests per second. Such findings point to the fact that the framework can be used to define the bottlenecks of performance and allow taking timely corrective measures aimed at enhancing the efficiency of the services. Moreover, the anomaly detection assessment allowed to establish that the suggested XAI-RA model exceeded the established machine-learning practices since it obtained 97.3% accuracy, 96.9% precision, 96.4% recall, and 96.6% F1-score. This proves that the framework does not only enhance the performance but also gives the cloud environments very reliable detection of anomaly. One of the key contributions of the presented work is the inclusion of explainable AI into the cloud reliability analytics. As it was shown in the SHAP-based explainability results, CPU usage, memory usage, and network-latency were the most impactful variables of the cloud performance anomalies. This is of particular significance since it converts the model into a black-box predictive system into a decision-support mechanism that is interpretable. The framework also lets the administrators and the engineers working on the site reliability know of the relative contribution of each of the system features to the degradation of the service, as well as the reason to validate the model results and make more optimized decisions. Thus, the suggested methodology enhances the technical performance as well as the trust, transparency, and operational usability. Scalability analysis also proved the appropriateness of the framework to large scale deployment to the cloud. The proposed system had steadily lower response times than the baseline framework up to workloads of 1000 and consistently higher throughput than the baseline framework up to workloads of 6000. The framework decreased response time by about 33.7 percent and throughput by almost 38.7 percent at peak load indicating high adaptability to the high demand conditions. These results indicate that scalable cloud service management may have a viable basis of dynamic and explainable reliability analytics. Altogether, the paper proves that explainability cannot be viewed as a nice-to-have feature of the cloud intelligence system, but as an essential precondition of a credible and efficient reliability engineering. The presented XAI-RA framework provides a balanced approach where predictive intelligence can be combined with interpretability, which is why this solution is highly applicable in the case of modern cloud infrastructures where the decisions regarding fault diagnostics, resource distribution, and performance optimization require accuracy and understanding. Irrespective of these contributions, there are some limitations of the study. The testing was done under a simulated cloud deployment and the findings should not then be considered as the complete deployment of the project in a database. Moreover, the framework concentrated more on the performance and reliability-based metrics, whereas the other significant areas of the performance, including cost-conscious optimization, energy efficiency, multi-cloud orchestration, and real-time security co-analysis were not investigated in depth. The next line of research can be done to support this study by validating the framework on actual cloud infrastructure, federated or online learning to update adaptive models, and more operational goals, like carbon-aware scheduling, zero-trust reliability analytics, and autonomous incident remediation. The additional extensions would enhance explainable AI applicability in the next-generation cloud service management.

References

1) B. Varghese and R. Buyya, “Next-generation cloud computing: New trends and research directions,” *Future Generation Computer Systems*, vol. 79, pp. 849–861, 2018.

2) M. U. Bokhari, Q. Makki, and Y. K. Tamandani, “A survey on cloud computing,” in *Big Data Analytics*. Springer, 2018, pp. 149–164.

3) S. S. Gill and R. Buyya, “Failure management for reliable cloud computing: A taxonomy, model, and future directions,” *Computing in Science & Engineering*, vol. 22, no. 3, pp. 52–63, 2020.

4) S. Taherizadeh and V. Stankovski, “Dynamic multi-level auto-scaling rules for containerized applications,” *The Computer Journal*, vol. 62, no. 2, pp. 174–197, 2019.

5) Manoj Kumar Kagitha, “COMPARATIVE ANALYSIS OF MACHINE LEARNING ALGORITHMS FOR PREDICTIVE ANALYTICS,” *GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES (GJESR)*, 3(12): December, pp. 99-108, 2016.

6) L. Tredinnick, “Artificial intelligence and professional roles,” *Business Information Review*, vol. 34, no. 1, pp. 37–41, 2017.

7) M. R. Belgaum, Z. Alansari, S. Musa, M. M. Alam, and M. S. Mazliham, “Role of artificial intelligence in cloud computing, IoT and SDN: Reliability and scalability issues,” *International Journal of Electrical and Computer Engineering*, vol. 11, no. 5, pp. 4458–4470, 2021.

8) W. Hummer *et al*., “ModelOps: Cloud-based lifecycle management for reliable and trusted AI,” in *Proc. IEEE Int. Conf. Cloud Engineering (IC2E)*, 2019, pp. 113–120.

9) J. Lee and J. Gil, “Adaptive fault-tolerant scheduling strategies for mobile cloud computing,” *The Journal of Supercomputing*, vol. 75, no. 8, pp. 4472–4488, 2019.

10) A. Das and P. Rad, "Opportunities and challenges in explainable artificial intelligence (XAI): A survey," *arXiv preprint arXiv:2006.11371*, 2020.

11) H. Liu, C. Zhong, A. Alnusair, and S. R. Islam, "FAIXID: A framework for enhancing AI explainability of intrusion detection results using data cleaning techniques," *Journal of Network and Systems Management*, vol. 29, no. 4, p. 40, 2021.

12) S. El-Sappagh, J. M. Alonso, S. R. Islam, A. M. Sultan, and K. S. Kwak, "A multilayer multimodal detection and prediction model based on explainable artificial intelligence for Alzheimer's disease," *Scientific Reports*, vol. 11, no. 1, p. 2660, 2021.

13) Manoj Kumar Kagitha, "OPTIMIZATION OF NEURAL NETWORKS USING GRADIENT DESCENT VARIANTS," *International Journal of Engineering Sciences & Management Research (IJESMR)*, 4(9): September, pp. 1-7, 2017.

14) L. Bittencourt *et al*., "The Internet of Things, fog and cloud continuum: Integration and challenges," *Internet of Things*, vol. 3, pp. 134–155, 2018.

15) J. I. R. Molano, J. M. C. Lovelle, C. E. Montenegro, J. J. R. Granados, and R. G. Crespo, "Metamodel for integration of internet of things, social networks, the cloud and Industry 4.0," *Journal of Ambient Intelligence and Humanized Computing*, vol. 9, no. 3, pp. 709–723, 2018.

16) M. Noura, M. Atiquzzaman, and M. Gaedke, "Interoperability in Internet of Things: Taxonomies and open challenges," *Mobile Networks and Applications*, vol. 24, no. 3, pp. 796–809, 2019.

17) Y. Zhang *et al*., "CloudRCA: A root cause analysis framework for cloud computing platforms," in *Proc. 30th ACM Int. Conf. Information & Knowledge Management*, 2021, pp. 4373–4382.

18) S. A. Javadi, R. Cloete, J. Cobbe, M. S. A. Lee, and J. Singh, "Monitoring misuse for accountable artificial intelligence as a service," in *Proc. AAAI/ACM Conf. AI, Ethics, and Society*, 2020, pp. 300–306.

19) E. Viegas, A. Santin, A. Bessani, and N. Neves, "BigFlow: Real-time and reliable anomaly-based intrusion detection for high-speed networks," *Future Generation Computer Systems*, vol. 93, pp. 473–485, 2019.

20) H. Karimipour, A. Dehghantanha, R. M. Parizi, K. R. Choo, and H. Leung, "A deep and scalable unsupervised machine learning system for cyber-attack detection in large-scale smart grids," *IEEE Access*, vol. 7, pp. 80778–80788, 2019.

21) Manoj Kumar Kagitha, "LOAD BALANCING TECHNIQUES IN DISTRIBUTED CLOUD ENVIRONMENTS," *JOURNAL OF CRITICAL REVIEWS (JCR)*, vol. 06, no. 01, pp. 608-613, 2019.

22) O. Hohlfeld, J. Kempf, M. Reisslein, S. Schmid, and N. Shah, "Scalability issues and solutions for software defined networks," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 12, pp. 2595–2602, 2018.

23) S. Song, H. Park, B. Choi, T. Choi, and H. Zhu, "Control path management framework for enhancing software-defined network reliability," *IEEE Transactions on Network and Service Management*, vol. 14, no. 2, pp. 302–316, 2017.

24) L. Xiao, X. Wan, X. Lu, Y. Zhang, and D. Wu, "IoT security techniques based on machine learning," *IEEE Signal Processing Magazine*, vol. 35, no. 5, pp. 41–49, 2018.

25) D. M. Wagner, "Scalable AI-driven cyber-physical systems for secure cloud and 5G networks: Predictive analytics, reliability, and sustainable energy integration," *International Journal of Engineering & Extended Technologies Research*, vol. 3, no. 5, pp. 3700–3708, 2021.

26) Manoj Kumar Kagitha, "GREENOPS IN THE CLOUD: AN AI-DRIVEN TELEMETRY ANALYSIS MODEL FOR REDUCING CARBON FOOTPRINT IN HIGH-AVAILABILITY CLUSTERS," *Journal of Computational Analysis and Applications (JOCAA)*, vol. 28, no. 06, pp. 140-162, 2020.

27) N. Taimoor and S. Rehman, "Reliable and resilient AI and IoT-based personalised healthcare services: A survey," *IEEE Access*, vol. 10, pp. 535–563, 2021.