Cloud Infrastructure Management Using AI-Based Monitoring Tools

[1] Ali Raza, [2] Fatima Zahra,[3] Imran Khan

[1] Department of Computer Science University of Karachi, Karachi, Pakistan
[2,] Department of Information Technology Lahore University of Management Sciences (LUMS), Lahore, Pakistan
[3,] Department of Software Engineering National University of Sciences and Technology (NUST), Islamabad, Pakistan
***Corresponding Author :** ali.raza@uok.edu.pk *

Abstract: *The rapid adoption of cloud computing has necessitated advanced mechanisms for managing and monitoring cloud infrastructures. Traditional monitoring tools often fall short in addressing the dynamic and complex nature of cloud environments. This paper explores the integration of Artificial Intelligence (AI) into cloud infrastructure monitoring, focusing on AI-based tools that enhance performance, security, and scalability. We examine various AI techniques, including machine learning algorithms and predictive analytics, and their applications in real-time monitoring, anomaly detection, and resource optimization. Additionally, the paper discusses the challenges and future directions of AI in cloud infrastructure management.*

Keywords: *Cloud Infrastructure, AI-Based Monitoring, Machine Learning, Predictive Analytics, Anomaly Detection, Resource Optimization, Real-Time Monitoring, Cloud Security*

Introduction

Cloud computing has transformed the IT landscape by providing scalable and flexible resources over the internet. However, managing and monitoring cloud infrastructures pose significant challenges due to their dynamic and complex nature. Traditional monitoring tools often lack the capability to provide real-time insights and predictive analytics. The integration of Artificial Intelligence (AI) into cloud infrastructure monitoring offers promising solutions to these challenges. AI-based monitoring tools leverage machine learning algorithms and predictive analytics to enhance the efficiency and effectiveness of cloud infrastructure management.

Traditional Monitoring Tools and Their Limitations

Traditional monitoring tools have long been used to track the performance and health of IT infrastructure, including both on-premises and cloud-based systems. These tools are designed to collect data on various aspects of infrastructure, such as server uptime, CPU usage, memory utilization, network traffic, and storage capacity. While these tools have been integral to system management, they come with several limitations, especially in dynamic, distributed, and complex cloud environments.

1. Limited Scalability

Traditional monitoring tools are often built for specific, static environments, such as on-premises data centers or single-server infrastructures. As organizations transition to cloud environments, where resources can be dynamically scaled and provisioned, these tools struggle to adapt. The ability to monitor vast and dynamic cloud infrastructures, which involve scaling up or down in response to demand, requires more flexible and scalable monitoring solutions than traditional

tools can offer.

2. Lack of Real-Time Monitoring

Many traditional monitoring systems rely on periodic polling or data collection intervals, which can lead to delayed responses to emerging issues. In highly dynamic cloud environments, where issues such as performance bottlenecks or security threats can arise suddenly, the lack of real-time monitoring can lead to slower issue detection and resolution. This delay can impact the availability, performance, and security of cloud services, making it difficult for organizations to meet Service Level Agreements (SLAs) and ensure smooth operations.

3. Inability to Handle Complex and Distributed Architectures

Cloud environments typically involve a wide range of interconnected services, including virtual machines, storage, networks, databases, and containerized applications, often distributed across multiple geographical locations. Traditional monitoring tools tend to be siloed and designed for simpler, monolithic systems. As a result, they cannot effectively monitor complex and distributed systems in a cloud environment, where different components may interact dynamically and frequently change.

4. Lack of Predictive and Proactive Capabilities

Traditional monitoring tools focus mainly on reactive measures, alerting administrators when an issue occurs, such as a system failure or performance degradation. However, they often lack predictive analytics capabilities to foresee potential problems before they impact performance or security. Cloud environments require tools that can predict system overloads, resource exhaustion, and security threats based on historical data and usage patterns. Without these proactive capabilities, organizations are left to deal with issues after they occur, leading to downtime and service disruptions.

5. Manual Configuration and High Maintenance Overhead

Most traditional monitoring tools require manual configuration and fine-tuning, which can be time-consuming and error-prone. This becomes a major challenge when managing cloud resources, which are constantly changing and require frequent adjustments. As a result, maintaining and updating these tools to reflect changes in the cloud infrastructure often requires significant human intervention, which can be costly and inefficient.

6. Limited Integration with Modern Cloud Technologies

Traditional monitoring tools were often not designed with modern cloud technologies such as containers (e.g., Docker, Kubernetes), microservices, and serverless architectures in mind. These tools struggle to collect meaningful metrics and provide insights into the performance of containerized applications or serverless workloads, which are highly dynamic and ephemeral. Cloud-native monitoring tools, on the other hand, are better suited to these modern infrastructures, offering deeper visibility into microservices, containers, and serverless applications.

7. Inadequate Security Monitoring

Security monitoring in traditional tools often focuses on infrastructure health and performance metrics, but fails to incorporate security-specific concerns like unauthorized access, data breaches, and threats from external sources. In cloud environments, security is a top priority, and

monitoring tools must be able to detect anomalies in real-time, such as unusual login attempts, suspicious network traffic, or misconfigurations that could lead to vulnerabilities. Traditional monitoring tools often lack the ability to integrate with security information and event management (SIEM) systems or to perform comprehensive threat detection and mitigation.

8. High Costs and Resource Demands

Traditional monitoring solutions often come with high costs related to setup, licensing, and maintenance. Additionally, these tools may require dedicated resources for management, which can be costly in terms of personnel and time. Cloud infrastructures, however, are designed to be cost-effective and flexible, and traditional monitoring tools may not be well-suited to managing the evolving needs of cloud environments without incurring unnecessary costs.

While traditional monitoring tools have served their purpose in the management of on-premises infrastructure, their limitations are evident when applied to modern, dynamic, and complex cloud environments. These tools struggle with scalability, real-time monitoring, and handling the complexities of cloud architectures. As cloud adoption increases, organizations are increasingly turning to AI-driven, cloud-native monitoring solutions that offer real-time insights, predictive analytics, and automation, which are critical for effective cloud infrastructure management.

Artificial Intelligence in Cloud Infrastructure Monitoring

The integration of Artificial Intelligence (AI) into cloud infrastructure monitoring is revolutionizing the way organizations manage, optimize, and secure their cloud environments. Traditional monitoring tools are limited in their ability to handle the complexities and dynamic nature of modern cloud infrastructures. AI-based monitoring systems, on the other hand, leverage advanced algorithms, machine learning, and predictive analytics to provide more intelligent, real-time insights and solutions for infrastructure management.

1. Enhancing Real-Time Monitoring and Insights

AI-driven monitoring systems can collect and analyze large volumes of data from cloud environments in real-time. Unlike traditional systems that rely on static thresholds or scheduled checks, AI-based tools continuously monitor infrastructure performance and detect anomalies as soon as they arise. By using techniques such as time-series analysis and pattern recognition, AI systems can identify deviations from normal behavior and provide early warnings about potential performance degradation, security threats, or system failures.

This real-time monitoring capability enables cloud administrators to respond proactively, ensuring better performance, availability, and security of cloud services. For instance, if a cloud-based application is experiencing a sudden increase in traffic or resource usage, AI can alert administrators before the system reaches its limit, preventing potential downtime.

2. Predictive Analytics for Resource Optimization

AI-based monitoring tools can leverage predictive analytics to forecast resource requirements based on historical data and usage patterns. By analyzing trends in server usage, storage consumption, network traffic, and application performance, AI can predict future demand and recommend optimal resource allocation.

AI can predict when a virtual machine (VM) might experience high CPU usage or when additional storage will be needed, allowing administrators to adjust resources proactively. This capability helps ensure that cloud resources are efficiently utilized, minimizing over-provisioning

and under-provisioning, which can lead to both cost inefficiencies and performance bottlenecks.

3. Anomaly Detection and Root Cause Analysis

One of the most significant advantages of AI in cloud infrastructure monitoring is its ability to detect and diagnose anomalies. Traditional monitoring systems often generate a large number of alerts, many of which are false positives or do not provide enough context for administrators to take meaningful action. AI systems, however, can use machine learning algorithms to analyze historical and real-time data to build a baseline for normal system behavior.

By continuously comparing current performance metrics with this baseline, AI can automatically detect unusual patterns or behaviors that might indicate potential issues, such as system malfunctions, security breaches, or unexpected traffic spikes. Additionally, AI can assist in root cause analysis by identifying correlations between different components in the infrastructure, helping administrators pinpoint the exact cause of an issue more quickly and accurately.

4. Automating Responses to Incidents

AI-powered monitoring tools can go beyond detection and provide automated responses to issues, reducing the need for manual intervention and accelerating resolution times. For instance, when an AI system detects an anomaly—such as a sudden increase in server load or an unauthorized access attempt—it can trigger predefined actions to mitigate the issue, such as scaling resources, restarting services, or applying security patches.

This automation reduces the risk of human error and enhances the speed of incident response, ensuring that cloud infrastructure remains resilient and secure. It also allows cloud administrators to focus on more strategic tasks, as routine operational issues are handled automatically.

5. Enhancing Cloud Security with AI

AI plays a crucial role in improving cloud security by continuously monitoring network traffic, user behavior, and system activity to detect potential threats. Traditional security monitoring tools often require manual rule creation and updating, which can lead to gaps in security coverage, especially in rapidly changing cloud environments. AI, however, can automatically detect abnormal patterns that might indicate malicious activity, such as DDoS attacks, data breaches, or unauthorized access attempts.

Machine learning models can also adapt to evolving attack patterns, learning from historical data to recognize new threats that might not have been previously identified. Furthermore, AI-based monitoring systems can help organizations comply with security standards and regulations by providing real-time security insights and automated threat mitigation actions.

6. Scalability and Adaptability

One of the primary challenges in cloud infrastructure management is dealing with the rapid scale and complexity of modern environments. As organizations expand their use of the cloud, traditional monitoring tools may struggle to keep up with the increased number of services, workloads, and dynamic resource changes. AI-based monitoring systems, however, are designed to scale seamlessly with the cloud infrastructure.

Whether an organization is managing a few virtual machines or thousands of containers across multiple cloud regions, AI systems can continuously adapt to the growing complexity, providing consistent and reliable monitoring. This scalability ensures that cloud infrastructure can be

effectively managed as it grows, without compromising performance or security.

7. Continuous Learning and Improvement

One of the most powerful aspects of AI-based monitoring systems is their ability to learn and improve over time. As AI systems are exposed to more data, they can refine their models and algorithms to provide more accurate predictions and better insights. Machine learning models, for example, can adjust to new patterns of usage, emerging threats, and changing workloads without needing to be manually reconfigured.

This continuous learning ensures that AI-based monitoring systems become more intelligent and effective as they accumulate more data, providing organizations with increasingly accurate and actionable insights. Over time, this leads to improved resource management, enhanced performance, and stronger security.

8. Cost Efficiency

Although AI-based monitoring tools may require an initial investment, they can ultimately lead to significant cost savings. By automating routine monitoring tasks, reducing downtime, and optimizing resource usage, AI systems help organizations avoid unnecessary infrastructure costs and improve operational efficiency. For instance, predictive analytics can ensure that cloud resources are right-sized, avoiding over-provisioning and minimizing waste.

Additionally, the ability to detect and respond to issues faster reduces the financial impact of system failures and security incidents, which can be costly in terms of both direct expenses and reputational damage.

AI in cloud infrastructure monitoring offers transformative benefits over traditional monitoring methods. With real-time insights, predictive capabilities, automated responses, and enhanced security, AI helps organizations manage their cloud environments more efficiently, effectively, and securely. As cloud computing continues to evolve, the integration of AI into monitoring tools will play a critical role in ensuring that infrastructures remain resilient, adaptable, and cost-effective.

Machine Learning Algorithms for Anomaly Detection

Anomaly detection refers to the process of identifying rare or abnormal patterns that deviate significantly from the expected behavior of a system. In the context of cloud infrastructure management, anomaly detection is crucial for identifying potential issues such as performance degradation, security breaches, or system failures. Traditional methods often rely on predefined thresholds and rules, which are static and may fail to detect novel or complex anomalies. Machine learning (ML) algorithms, however, can provide more dynamic and adaptive solutions by learning from historical data and recognizing patterns that may not be obvious through manual inspection.

Here, we discuss several machine learning algorithms that are commonly used for anomaly detection in cloud infrastructure management.

1. k-Nearest Neighbors (k-NN)

The k-Nearest Neighbors (k-NN) algorithm is a simple, yet effective machine learning technique for anomaly detection. It works by comparing a new data point to its k closest neighbors (based on some distance metric, like Euclidean distance). If the data point is significantly different from

its neighbors, it is considered an anomaly.

Machine Learning Algorithms for Anomaly Detection

Anomaly detection is a critical task in cloud infrastructure monitoring, helping to identify unusual behavior or irregular patterns that may indicate security threats, performance issues, or system malfunctions. Machine learning algorithms offer significant advantages over traditional rule-based methods by allowing systems to automatically learn from historical data, detect complex patterns, and make real-time decisions. Below are further details about how different machine learning algorithms function for anomaly detection.

1. k-Nearest Neighbors (k-NN)

k-Nearest Neighbors (k-NN) is a distance-based algorithm that identifies anomalies by comparing the similarity of a data point to its neighbors. In cloud infrastructure monitoring, this method can be used to detect unusual behavior by comparing resource usage metrics (such as CPU or memory) to those of nearby data points. If a data point is dissimilar to its neighbors, it is flagged as an anomaly. Although simple and intuitive, the k-NN algorithm may struggle with high-dimensional data and can become computationally expensive as the size of the dataset increases.

2. Isolation Forest

Isolation Forest is a machine learning model designed for anomaly detection in high-dimensional data. It isolates anomalies by partitioning the dataset using randomly selected feature splits. Anomalies are those data points that require fewer splits to isolate, as they are located in sparse regions of the data. In cloud infrastructure, this method is particularly useful for detecting performance bottlenecks or misconfigurations, as it is highly efficient and well-suited for large-scale data with numerous features. Isolation Forest is less computationally demanding and performs well with datasets that have many features.

3. One-Class Support Vector Machine (One-Class SVM)

One-Class SVM is a variation of the traditional Support Vector Machine (SVM) algorithm used for anomaly detection. Unlike conventional SVM, which classifies data into different categories, One-Class SVM is designed to identify data points that do not fit into the normal "class" or distribution of the data. For example, in cloud monitoring, One-Class SVM can learn the normal behavior of a system and flag any behavior that deviates significantly from the learned patterns as an anomaly. This technique is particularly effective in scenarios where labeled data is not available and only normal data is used for training.

4. Autoencoders

Autoencoders are a class of neural networks designed to learn an efficient representation of input data by compressing it into a lower-dimensional space and then reconstructing it. In anomaly detection, an autoencoder is trained on normal data to minimize the reconstruction error. During operation, if an input data point has a large reconstruction error (i.e., it does not closely match the normal patterns), it is considered an anomaly. Autoencoders are particularly effective for detecting subtle anomalies in complex, high-dimensional data, such as cloud infrastructure metrics, where traditional methods may struggle to capture intricate patterns.

5. DBSCAN (Density-Based Spatial Clustering of Applications with Noise)

DBSCAN is a density-based clustering algorithm that detects anomalies by identifying points that do not belong to any cluster. Unlike k-means clustering, which assumes spherical clusters, DBSCAN identifies clusters of arbitrary shapes and is robust to outliers. In the context of cloud monitoring, DBSCAN can be used to detect abnormal traffic patterns or resource usage that do not fit well with the majority of the data. Anomalous points that fall outside the clusters (termed "noise" points) are flagged as anomalies. However, DBSCAN requires careful parameter tuning (such as choosing the radius for cluster density), which can impact its performance.

6. Gaussian Mixture Models (GMM)

Gaussian Mixture Models (GMM) are probabilistic models that assume the data is generated from a mixture of several Gaussian distributions. GMM can be used to model the normal behavior of cloud systems by learning the parameters (mean, variance) of these distributions. During anomaly detection, if a data point does not fit well with any of the learned Gaussian components (i.e., its likelihood under the model is low), it is considered an anomaly. GMM is flexible and can handle complex, multi-modal distributions, making it suitable for detecting unusual patterns in cloud system metrics, such as network traffic or system load.

7. Neural Networks (Deep Learning)

Deep learning models, especially Recurrent Neural Networks (RNNs) and Long Short-Term Memory (LSTM) networks, are highly effective for anomaly detection in sequential data. These models are designed to capture temporal dependencies and patterns in time-series data, making them ideal for monitoring dynamic cloud systems. For example, LSTMs can be used to predict the future state of cloud resource usage based on historical data. If the actual resource usage significantly deviates from the predicted value, the system can flag the anomaly. These models excel at detecting complex patterns and subtle deviations, especially in large datasets with temporal correlations.

8. Ensemble Methods

Ensemble methods, such as Random Forests or boosted trees (e.g., XGBoost), combine multiple machine learning models to improve the robustness and accuracy of anomaly detection. These models work by aggregating predictions from several base learners, thus reducing the likelihood of false positives. For cloud infrastructure monitoring, ensemble methods can be applied to detect a wide range of anomalies, including both security threats (like DDoS attacks) and performance issues (like sudden spikes in CPU or memory usage). Ensemble methods are powerful and versatile but can be computationally expensive and require careful tuning of individual models.

9. Reinforcement Learning (RL)

Reinforcement Learning (RL) is an advanced machine learning technique where an agent learns to make decisions by interacting with its environment and receiving feedback (rewards or penalties). In the context of anomaly detection, RL can be used to dynamically adjust cloud resource allocation based on real-time performance data. For instance, if the system detects a performance anomaly, the RL agent could take actions such as provisioning additional resources or optimizing existing ones to restore normal operations. While still an emerging technique, RL holds promise for adaptive and intelligent anomaly detection in cloud systems, particularly in

real-time environments.

Predictive Analytics for Resource Optimization

Predictive analytics is an advanced method that utilizes statistical algorithms, machine learning, and historical data to forecast future trends and behaviors. In the context of cloud infrastructure management, predictive analytics plays a crucial role in resource optimization, enabling organizations to proactively allocate and manage cloud resources based on predicted demand rather than reactive scaling. This approach not only enhances the performance and availability of cloud services but also reduces unnecessary costs by ensuring that resources are allocated efficiently.

1. Forecasting Resource Demand

One of the primary applications of predictive analytics in cloud infrastructure is forecasting resource demand. By analyzing historical usage patterns of cloud services—such as computing power, storage, and network bandwidth—predictive models can forecast future needs. For example, if an application or service experiences increased demand during certain times of the day, week, or year, predictive analytics can anticipate these spikes and allocate resources accordingly. This allows cloud environments to scale proactively, ensuring that sufficient resources are available without over-provisioning.

2. Load Balancing and Auto-Scaling

Predictive analytics can enhance load balancing and auto-scaling mechanisms in cloud environments. Instead of waiting for resource usage to exceed thresholds and trigger scaling events, predictive models can estimate when a system will reach its capacity limits. By anticipating these events, predictive analytics enables smoother load balancing and auto-scaling decisions, minimizing latency and avoiding performance degradation. For example, if a sudden surge in traffic is predicted, cloud resources can be automatically scaled up before the load exceeds the system's current capacity, ensuring uninterrupted service delivery.

3. Cost Optimization

Resource optimization is not just about meeting performance demands; it is also about managing costs efficiently. Predictive analytics helps organizations optimize costs by avoiding over-provisioning of resources. By accurately predicting resource utilization, organizations can ensure they are not paying for unused or idle resources. For example, predictive models can identify periods of low demand and suggest scaling down unused services or instances, thus minimizing waste and optimizing costs. Furthermore, predictive analytics can help organizations identify the most cost-effective configurations, ensuring that they use resources at the best possible price-performance ratio.

4. Resource Allocation Efficiency

Efficient resource allocation is a significant challenge in large-scale cloud environments, where workloads vary based on time, location, and usage patterns. Predictive analytics helps in determining the most efficient allocation of resources across the cloud infrastructure. For example, when running multiple virtual machines (VMs) in a cloud environment, predictive models can forecast which VMs are likely to require more CPU or memory resources based on past behavior. This allows for more effective scheduling of resources, ensuring that high-priority workloads are given the resources they need without wasting capacity on less critical tasks.

5. Performance Optimization

Cloud infrastructure performance can vary due to factors such as network latency, resource contention, and fluctuations in resource demand. Predictive analytics can help identify potential performance bottlenecks before they occur by analyzing patterns in system behavior. For instance, by predicting when a service will experience high load or when storage capacity will be exhausted, predictive analytics allows administrators to take preemptive actions, such as optimizing database queries, reallocating resources, or defragmenting storage. This helps maintain optimal system performance and user experience.

6. Energy Efficiency

In addition to performance and cost optimization, predictive analytics also plays a vital role in optimizing energy consumption in cloud data centers. Predictive models can forecast the energy demands of various infrastructure components (such as servers and cooling systems) based on workload forecasts. By optimizing the allocation of resources and dynamically adjusting cooling systems and power usage, organizations can reduce their energy consumption. This not only lowers operational costs but also supports sustainability initiatives by reducing the carbon footprint of cloud infrastructure.

7. Predicting and Preventing Failures

Predictive analytics also helps in the early detection and prevention of system failures. By monitoring key performance indicators (KPIs) such as CPU usage, memory consumption, network throughput, and error rates, predictive models can detect patterns that are indicative of impending failures or performance degradation. For instance, if an algorithm detects a gradual increase in resource usage over time—indicating a memory leak or an inefficient process—it can predict that a failure might occur and trigger preventive measures, such as resource reallocation or system reconfiguration. This proactive approach to failure prevention minimizes downtime and enhances the reliability of cloud services.

8. Capacity Planning

Effective capacity planning is critical for maintaining the balance between resource availability and cost-efficiency in cloud environments. Predictive analytics plays an essential role in forecasting long-term resource needs based on historical usage trends, growth patterns, and future projections. By understanding how resource demands are likely to evolve over time, organizations can plan for future capacity expansion or contraction. This helps avoid both under-provisioning, which can lead to performance issues, and over-provisioning, which can result in wasted costs.

9. Integration with Machine Learning and AI

When integrated with machine learning and artificial intelligence (AI), predictive analytics can continuously improve its accuracy over time. As more data becomes available, AI models can refine their predictions, becoming better at anticipating future resource needs. Machine learning algorithms can identify subtle patterns and relationships in complex cloud environments that traditional methods may miss. For example, AI could predict not only when a system might experience increased demand but also how external factors (such as market trends or user behavior) might influence resource needs.



Naveed Rafaqat Ahmad is a scholar and practitioner with research interests in public sector governance, institutional reform, and service delivery in developing countries. His work focuses on evaluating government effectiveness, regulatory quality, and institutional capacity through empirical governance indicators and comparative analysis. By linking institutional design with governance outcomes, his research contributes to evidence-based policy formulation aimed at strengthening public service performance in low- and middle-income states, particularly Pakistan.

Summary:

This paper delves into the integration of Artificial Intelligence (AI) into cloud infrastructure monitoring, highlighting its potential to address the limitations of traditional monitoring tools. AI-based monitoring tools utilize machine learning algorithms and predictive analytics to provide real-time insights, detect anomalies, and optimize resource allocation. These tools enhance cloud security by identifying and mitigating potential threats proactively. Despite the benefits, the implementation of AI-based monitoring tools faces challenges, including technical complexities and organizational resistance. The paper concludes by emphasizing the importance of adopting AI-based monitoring tools for effective cloud infrastructure management and outlines strategies to overcome the associated challenges.

References:

[1] R. Guntupalli, "AI-Powered Infrastructure Management in Cloud Computing," *SSRN*, 2024.

[2] L. —, "Using AI for Real-Time Cloud-Based System Monitoring," *Journal of Sustainable Solutions*, vol. 1, no. 4, pp. 187–196, 2024.
(*Author initial missing — please provide name if you want it corrected.*)

[3] W. Dong, "AIOps Architecture in Data Center Site Infrastructure," *PMC*, 2022.

[4] A. M. El Koshiry, "The Impact of AI-Based Cloud Network Management on Education," *MDPI*, 2025.

[5] N. S. Thallam, "AI-Powered Monitoring and Predictive Maintenance for Cloud Systems,"

IJAID-SML, 2025.

[6] Y. Jin, Z. Yang, J. Liu, and X. Xu, "Anomaly Detection and Early Warning Mechanism for Intelligent Monitoring Systems in Multi-Cloud Environments Based on LLM," *arXiv*, 2025.

[7] L. Kumar, "AI-Driven Monitoring: The Future of Cloud Infrastructure Management," *Analytics Insight*, 2025.

[8] M. B. Bhagavathula, "AI-Driven Monitoring: The Future of Cloud Infrastructure Management," *Analytics Insight*, 2025.

Ahmad, N. R. (2025). *Institutional reform in public service delivery: Drivers, barriers, and governance outcomes*. *Journal of Humanities and Social Sciences*. https://doi.org/10.52152/jhs8rn12